Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods

Nele Borgert
nele.borgert@rub.de
Ruhr University Bochum
Bochum, Germany

Luisa Jansen
luisa.jansen@rub.de
Ruhr University Bochum
Bochum, Germany

Imke Böse
imke.boese@rub.de
Ruhr University Bochum
Bochum, Germany

Jennifer Friedauer
jennifer.friedauer@rub.de
Ruhr University Bochum
Bochum, Germany

M. Angela Sasse
martina.sasse@rub.de
Ruhr University Bochum
Bochum, Germany

Malte Elson
malte.elson@rub.de
Ruhr University Bochum
Bochum, Germany

ABSTRACT

Amidst growing IT security challenges, psychological underpinnings of security behaviors have received considerable interest, e.g. cybersecurity Self-Efficacy (SE), the belief in one's own ability to enact cybersecurity-related skills. Due to diverging definitions and proposed mechanisms, research methods in this field vary considerably, potentially impeding replicable evidence and meaningful research synthesis. We report a preregistered systematic literature review investigating (a) cybersecurity SE measures, (b) SE's proposed roles, and (c) intervention approaches. We minimized selection bias by detailed exclusion criteria, interdisciplinary search strategy, and double coding. Among 174 cybersecurity SE studies (2010-2021) from 18 databases with 55,758 subjects, we identified 173 different SE measures with considerable differences in psychometric quality and validity evidence. We found 276 variables as assumed causes/outcomes of cybersecurity SE and identified 13 intervention designs. This review demonstrates the extent of methodological and conceptual fragmentation in cybersecurity SE research. We offer recommendations to inspire our research community toward standardization.

CCS CONCEPTS

• **Human-centered computing** → **HCI design and evaluation methods**; • **Security and privacy** → *Human and societal aspects of security and privacy*.

KEYWORDS

Self-Efficacy, Cybersecurity, Systematic Review, Research Methods

ACM Reference Format:
Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M. Angela Sasse, and Malte Elson. 2024. Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 32 pages. https://doi.org/10.1145/3613904.3642432

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/ 24/05.
https://doi.org/10.1145/3613904.3642432

1 INTRODUCTION

1.1 Cybersecurity Self-Efficacy

Data privacy and usable IT security are increasingly becoming concerns of public interest as a result of (a) the ever-growing presence of IT products in average consumer households, and (b) the amounts and immense value of personal data they process. However, protection of personal data is as much a technical challenge as it is a psychological one [20, 120], which is why usable security research has increasingly focused on improving security-related behaviors of individual users [3, 72, 152, 160]. A key starting point from motivational psychology for influencing IT security behaviors is a person's cybersecurity Self-Efficacy (SE). SE is defined as the belief about one's own ability to enact certain skills [23]. Its high relevance for behavior through motivational, cognitive, emotional, and choice-related processes [23, 26] has put it on the map of Human-Computer Interaction (HCI) researchers [e.g., 35, 129, 141]. As indicated by an evidence review featured in the [59] report, self-efficacy stands as the sole factor on the human side that consistently predicts cybersecurity intention and behavior.

The interdisciplinary nature of cybersecurity SE research has led from a "general scarcity of theoretical models to guide IT researchers" [77, p. 526] to broad construct definitions across scientific disciplines and communities, and in consequence, a blurred terminology of self-efficacy has emerged: privacy self-efficacy [168], coping self-efficacy [149], computer self-efficacy [111], internet self-efficacy [55], self-efficacy in information security [129], security self-efficacy [113], cybersecurity SE [18], self-efficacy to comply with information security policy [34], and more. Hence, there is a risk that the cybersecurity SE literature suffers from the jingle-jangle fallacy [65]: The jingle fallacy refers to the belief that two instruments measure the same constructs because they share a similar name, whereas a jangle fallacy would be the similarly incorrect belief that differently named instruments indeed measure distinct constructs [65]. Both fallacies affect the validity of interpretations of an empirical literature [103, 161] as they obfuscate the true coherence (or lack thereof) of (seemingly) related concepts. We argue that before attempting to collate empirical evidence for substantive research questions in this field (e.g., "Does cybersecurity SE predict security behaviors?"), it is essential to understand and evaluate methodological characteristics of that evidence that could increase risk of bias [cf. 123].

This work systematically assesses the methodological heterogeneity in primary studies in the field of cybersecurity SE. Specifically, we examine reported measures of cybersecurity SE, the underlying theoretical assumptions of the role of cybersecurity SE, as well as designed interventions to support cybersecurity SE. This research could be used in future work, for example, to inform subsequent systematic reviews or meta-analyses on empirical evidence. Despite this study being about methodology rather than research outcomes, we use process elements that are common in substantive reviews, such as structured systematic search and study screening [cf. 153].

2 RELATED WORK

2.1 Background and Contribution

Efforts have been made to gain clarity about the concept of cybersecurity SE and to consolidate the rather fragmented literature. He et al. [76], for example, conducted a literature review and found 13 different cybersecurity SE measures with inconsistent terminology, item wording, and construct facet coverage (i.e., instruments were sometimes omitting aspects of cybersecurity SE relevant to measure the construct holistically). Besides the recommendation to provide a clear definition of cybersecurity SE, they advise considering all dimensions of cybersecurity SE when constructing a scale to ultimately achieve consistent operationalization across studies.

There is reason to believe that research in this field has not heeded He et al.'s [76] call toward a more consistent methodology. Publications continue to draw on incoherent cybersecurity SE definitions and measures, both within and across research disciplines. Especially, since widely discussed security incidents seem to have motivated an inflated use of self-efficacy (and derivatives of it) without prior standardization or coherent theory development. We strive to address the current expansion of the field's knowledge base by assessing the heterogeneity in cybersecurity SE research methods in HCI almost a decade after He et al.'s [76] review was published.

More recent HCI reviews on cybersecurity research do usually not thoroughly consider methodological standardization of SE measurement. Some reviews focus on specific populations, applications, contexts, or venues: Akinrotimi [8] reviewed educational tools for students with $N = 2$ studies involving SE; Sari et al. [140] investigated healthcare staff or patients and found SE to be the most frequently studied human factor ($N = 12$); Quayyum et al. [124] conducted a review on children and identified $N = 2$ studies resorting to SE approaches; AL-Nuaimi [9] reviewed security behavior in organizations and found $N = 3$ studies investigating the influence of self-efficacy; Chowdhury et al. [42] considered the influence of time pressure and counted $N = 4$ papers regarding SE; and Rohan et al. [133] conducted a review limiting their search strategy to one human factor conference outlet and located $N = 2$ studies on SE. Our review covers a variety of interdisciplinary databases while transparently recording framework and sample details to assess research methodology across the entire field of cybersecurity SE studies in HCI.

There are also substantial review contributions that survey the relationship between particular constructs (e.g., Alshammari et al. [12] report the prevalence of studies on SE, $N = 5$, within protection behavior research on emotions; Reddy and Dietrich [128] focus on the role of SE for security compliance, $N = 14$, and include a methodological comparison between self-reports and non-self-reports attempting to clarify inconsistent findings). Other reviews in the field of HCI investigate practical implications of SE theories by assessing sources of cybersecurity SE. For example, Zhang-Kennedy and Chiasson [170] looked at intervention tools and found $N = 1$ study that examined narrative learning materials and their benefit to SE, Jones et al. [90] reviewed design recommendations for warning messages to increase SE with $N = 1$ study, Coenraad et al. [45] surveyed games to promote SE and focused on the content of the learning materials, and Jeong et al. [88] highlight with $N = 1$ study the importance of tailored interventions especially with regard to different SE levels. Further, there are also reviews on SE theories themselves. Sulaiman et al. [154] present the most referred-to theories in cybersecurity compliance research in organisations, some of which involve SE as a determinant, and Maalem Lahcen et al. [109] consider relevant theories specifically for cybersecurity behavior where SE is mentioned regarding Social Cognitive Theory.

Broad reviews on cybersecurity behavior demonstrate the current research interest in SE's influence: Almansoori et al. [11] find SE to be the most frequent external factor, i.e., viewing SE not as part of an original theory, for security behavior with $N = 16$ studies; Alsharida et al. [13] identify SE as the most common determinant of security behavior with $N = 37$ studies, but do not consider methodological aspects of this body of work. Prior to our review, this was accomplished either within meta-reviews (e.g., Khan et al. [93] take note of SE solely in organizational settings ($N = 4$) but assess review methodology) or other research fields [e.g., 66, 96, 164].

2.2 Review Goals

In this preregistered literature review, we aim to systematically assess the extent of heterogeneity in cybersecurity SE research methods, with a particular focus on:

- Goal 1 – reported self-efficacy measures and their psychometric quality criteria,
- Goal 2 – the role of self-efficacy within its theoretical assumptions, and
- Goal 3 – implemented interventions designed to support cybersecurity SE.

Each goal aligns with a specific research question, detailed in the following sections. In achieving our goals, we hope to raise awareness regarding heterogeneous research practices and aspire to encourage a shift towards greater consistency in measures, theories, and interventions within the realm of cybersecurity SE.

2.3 Measuring Cybersecurity Self-Efficacy

A prerequisite for meaningful research synthesis is standardization of empirical procedures and measures which ensures comparability of studies and adequate inferences from systematic reviews of the evidence [57].

Bandura [25, 27] proposed guidelines for self-efficacy measures. First and foremost, self-efficacy is a domain-specific characteristic, and consequently, items in self-report instruments need to reflect

behaviors and experiences specific to an activity domain. For content validity, self-efficacy items need to be formulated with "can do" statements and be distinguishable from other closely related constructs, such as competence [130], hope and optimism [126], locus of control [150], or outcome expectation [77]. The domain specification of self-efficacy beliefs demands prior assessment of controllable and multicausal behavioral factors required to succeed in the activity of interest. The granularity of self-efficacy, as well as challenges and impediments, such as self-regulatory task demands, differentiate between negligible and highly efficacious beliefs. The item analysis (pretesting, factor analysis, and reliability computation) as well as validation process (face, discriminant, and predictive validity) are also outlined to establish an easy access to standard quality criteria.

Ambiguities of measures jeopardize study comparability and valid inferences from a research literature [65], whereas insights about methodologies notably facilitate the synthesis of related studies and reconciliation of conflicting outcomes [57]. In achieving goal 1 (assessing measurement heterogeneity), we hope to encourage a shift towards greater consistency in cybersecurity SE measures [cf. 162]. Thus, this review examines information on scale development, scale structure, item wording, reliability as well as validity (content, construct, criterion, and incremental):

RQ1: What measures are used to assess cybersecurity self-efficacy? What are their scale characteristics and reported psychometric properties?

2.4 The Role of Cybersecurity Self-Efficacy

Inconsistencies of measures can be rooted in the differences between theoretical approaches and understandings of self-efficacy. Research involving cybersecurity SE may attribute different effect pathways to SE based on different theoretical assumptions. In Social Cognitive Theory [22], SE functions as a key construct that predicts human motivation, emotion, and actions more accurately than their actual abilities, knowledge, or skills [23]. Ajzen's [7] Theory of Planned Behavior understands SE as part of perceived behavioral control, which affects behavioral performance jointly with an individual's intentions to perform that action. Self-Determination Theory [50] on the other hand, postulates self-efficacy to be an even more distal factor that influences actions indirectly through its effects on self-determined motivation, and assigns autonomy the more important role in determining behavior [155].

Because SE is a relevant construct in IT security and privacy research, it has been studied from various angles. Reflecting different conceptualizations of self-efficacy itself, other theories frequently used in IT security research also differ in their understanding of SE as a determinant of human behavior. The Health Belief Model [134, 135] sees SE as a direct influence on the probability of preventive behavior, whereas a current revision of the Protection Motivation Theory [118] highlights the role of biases, norms, and a sense of responsibility in decision-making processes that, together with SE, have a mediated effect on protective behavior by intentions, i.e., one's protection motivation [132].

This entails a wide range of factors as causes or outcomes of SE that are of high interest to effectively motivate and predict behavioral change in users' cybersecurity. In this review, we aim to assess the heterogeneity of cybersecurity SE's role within its theoretical assumptions in empirical research (see goal 2). Understanding on this level is most critical to identify prevailing theoretical assumptions and assess the current stage of theory assertiveness of the nomological network cybersecurity SE is integrated within. Therefore, our second research question is as follows:

RQ2: What role does cybersecurity self-efficacy play in the theoretical or research models of empirical research?

2.5 Cybersecurity Self-Efficacy Interventions

An inconsistent theoretical understanding of self-efficacy in research models would lead to a multitude of potential directions for the design of interventions to support cybersecurity SE. Bandura [21, 22] outlines SE as a belief which can be changed, and strengthened, by (a) mastery experience, (b) vicarious experience, (c) persuasion, and (d) emotional arousal. Mastery experience revolves around one's own performance accomplishments induced either by self-modeling, performance desensitization, performance exposure, or self-instructed performance. However, observing other people perform a behavior of interest, e.g. via live or symbolic modeling, can also build another individual's SE vicariously. A rather weaker source of information is persuasion, which can be achieved through social or verbal suggestion, exhortation, interpretive treatments, or self-instruction. And finally, emotional arousal is in part judged as a physiological feedback for one's level of stress and anxiety. If highly aroused, people do not expect successful coping and accordingly, adjust their self-efficacy belief. This source of expectation can be influenced by attribution, relaxation and biofeedback, symbolic desensitization, or symbolic exposure, but it is not always highly reliable. These sources point to potential key aspects of SE interventions, but importantly, it is behavioral information that foster the necessary belief in one's own abilities [21].

The general difficulty to influence security behaviors might be rooted in the nature of IT security tasks. Those tasks usually compete with other more salient and relevant goals for which the utilized systems were implemented for, e.g., its convenience functions such as email communication or sharing files. Meaning that for most users, handling security settings is seen as secondary and foremost challenging [29]. Given these challenges of cybersecurity interventions, we need particularly reliable methods that have consistently proven to support usable IT security.

In this review, our third goal is to assess the heterogeneity of intervention designs that support cybersecurity SE. Even though measures and theories might not be uniform and consistent, this review's intention is not to dismiss promising scientific contributions of interventions; on the contrary, in achieving goal 3, we aspire to encourage a shift towards greater consistency in cybersecurity SE interventions. A more standardized methodological approach to cybersecurity SE interventions is crucial with regard to the construct's validation as well as instrumental for practitioners. This motivated our third research question of this review:

RQ3: Do the studies report interventions that have been carried out to manipulate cybersecurity self-efficacy? If so, what was their approach?

In summary, this review examines measures of cybersecurity SE and reported psychometric quality criteria (see goal 1), cybersecurity SE's role within its theoretical assumptions (see goal 2), and interventions that are designed to support cybersecurity SE (see goal 3). We conducted a systematic literature search that aims to assess the extent of heterogeneity of these methodological aspects.

3 METHODS

3.1 Preregistration

This review paper is part of an overarching project preregistered on the OSF (OSF registration link: anonymous preregistration) prior to data collection. In addition, we follow the international PROSPERO scheme (OSF file link: PROSPERO scheme) for documentation standards of systematic review protocols for research with human subjects, and report our findings in compliance with the PRISMA guidelines (OSF file link: PRISMA guidelines) for transparent reporting of systematic reviews and meta-analyses.

3.2 Selection Criteria

We included any empirical research published in English language (regardless of where the studies were conducted).

Since the review focuses on cybersecurity SE, we only included studies on the relationship between self-efficacy and IT security or privacy. Studies on self-efficacy in other contexts, or IT security/privacy without a link to self-efficacy were excluded. To this end, studies for inclusion had to specify the (hypothesized) importance of self-efficacy to IT security or privacy. We incorporated both qualitative and quantitative research as long as they included some measure of self-efficacy. Studies with experimental manipulations designed to affect cybersecurity SE were also included.

We included studies published between January 1, 2010 and March 18, 2021. We chose this timeframe to capture studies with modern IT devices and therefore modern cybersecurity.

3.3 Literature Search

To account for the interdisciplinariness of the literature, our search strategy covered a total of 18 electronic databases: ACM Digital Library, arXiv, dimensions.ai, EBSCOhost (incl. Academic Search Premier, APA PsycArticles, APA PsycInfo, Historical Abstracts, OpenDissertations, PSYNDEX Literature with PSYNDEX Tests), IEEE Xplore, Science Direct, Scopus, Web of Science (incl. WOS, KJD, MEDLINE, RSCI, SCIELO), and Wiley Online Library. These databases were selected to (a) cover relevant material of the diverse disciplines, (b) include grey literature, i.e. records released outside publishing houses including non-peer-reviewed sources, as well as late breaking work, and (c) exclusively rely on reproducible engines.

The syntax of our search string used an AND-connector to combine self-efficacy with IT security and privacy terms, whereas OR-connectors separated those somewhat synonymous terms. Our aim was to compile an exhaustive list of search terms covering the omnifaceted spectrum of relevant content, including technical, social, and psychological aspects of cybersecurity SE. Hence, keywords for IT security and privacy were generated in a two-step process. First, field experts were asked to list search terms as relevant as possible fitting in this concept group without generating too ambiguous keywords. Second, to combat a potentially biased search string, we relied on a quasi-automated method that uses text mining and keyword co-occurrence networks to suggest further IT security and privacy terms. This method is implemented in the R package litsearchr [70] (R version: 4.0.3; package version: 1.0.0). Our two-step approach ensured a thorough and reproducible search strategy. The general keyword string was:

> "self-efficacy" AND ("cybersecurity" OR "cyber security" OR "information security" OR "IT security" OR "information technology security" OR "IS security" OR "information system security" OR "wireless security" OR "home wireless security" OR "usable security" OR "computer security" OR "data protection" OR "data security" OR "personal data" OR "privacy" OR "security threat" OR "wireless network" OR "device security").

For each specific search string that was applied in the respective database, see preregistration files in our OSF project (OSF file link: search terms). Hits discovered just by matches of our search string in the full text, but not in the combined abstract, title, and keywords, were excluded, as cybersecurity SE was unlikely to be an important variable in the paper. EBSCOhost was the only database that could not be specifically restricted to an abstract, title, and keyword search, but instead matched the search string with a full text search. Hence, we used a custom Python script (OSF file link: search improvement script) which allowed identifying hits that were failing the search string in their combined abstracts, title, and keywords.

3.4 Study Selection

Data collection occurred March 18, 2021. In total, all database searches identified 1769 records of interest. The chronological sequence of import into Citavi (Build Number: 6.4.0.35) is presented in Table 1. Of 376 EBSCOhost hits, the Python script identified 201 false positives. Removing duplicates yielded a total of 696 records to be screened in the title sift.

Figure 1 illustrates a flow diagram summarizing the study selection process. We conducted three separate sifts to iteratively implement the pre-determined selection criteria: (1) a title, (2) an abstract, and (3) a full text sift. The reasons for exclusion were recorded for each record. During title sift, 134 records were excluded, leaving 562 records to be screened in the abstract sift. Here, another 276 documents were excluded, leaving 286 records for the full text sift. The third sift excluded additional 117 documents, and one record was excluded during the coding phase.

Consequently, 168 remaining records were eligible and included in the synthesis. Regarding publication information, the mode of publication year was $m_{\text{year}} = 2020$. The final sample split into 107 journal articles, 39 conference papers, 17 dissertations, 3 conference proceedings, 1 book chapter, and 1 report. Of these publications, 131 (77.98%) were peer-reviewed, 19 (11.31%) were not peer-reviewed, and another 18 (10.71%) publications did not provide information about the review process. See Appendix A for split analyses of differences between peer-reviewed and non-peer-reviewed records. In context of the sample description, these publications stem from various cultural backgrounds and represent 30 countries (at least 44.81% from USA, followed by 7.65% from Malaysia). Their combined sample size totals 55,758 study participants (53,586 study participants

Table 1: Sequence of Import into Citavi

Step	Meta Database	Hits	Duplicates Removed	Titles
1	arXiv	5	–	5
2	IEEE Xplore	57	0	97
3	ACM Digital Library	22	0	42
4	Science Direct	209	89	120
5	dimensions.ai	402	134	339
6	Scopus	290	207	120
7	Web of Science	316	242	74
8	Wiley Online Library	25	15	10
9	EBSCOhost	448[1]	168	210[2]

Note. [1]Including 72 exact duplicates removed by EBSCOhost; [2]Prior to custom Python script implementation.

when accounting for assumed sample duplicates) with a mean sample size of $M_{\text{size}} = 313.25$ ($SD = 250.61, MD_{\text{size}} = 249$), ranging between 4 and 1663 study participants. The median age weighted by sample size was $MD_{\text{age}} = 32.98$. For $N = 47,109$, we calculated a gender distribution weighted by sample size of 50.05% male, 49.49% female, 0.02% non-binary, and 0.21% no response. 30.05% of the studies reportedly used student samples. Samples were primarily recruited within organizations (51.37%), 22.95% via online panels, 13.66% recruited their samples ad-hoc, 6.01% had mixed recruitment strategies, and 6.01% did not describe recruitment. Concerning study information, the publications include 174 studies (142 surveys, 16 experiments, 6 quasi-experiment, and 10 studies of other types), 55.17% of which were conducted online, 25.29% were physical studies, 7.47% had mixed settings, under one percent were conducted via phone, and 11.49% did not report the study setting.

During the full paper sift and coding, 11 cases were excluded after group discussion: (a) multi-item self-efficacy scales containing only a single item or few items related to cybersecurity [71, 82, 83, 163] were not considered further because they are more indicative of confounding cybersecurity elements within a different construct in focus rather than fulfilling the requirements to be classified as a measure of cyberseucrity SE, and (b) we excluded studies studying cybersecurity SE of practitioners [16, 28, 79, 107, 144, 146] or hackers [108], rather than end users aiming to accomplish IT security or privacy. The group discussion was initiated by coders identifying some of these borderline cases, where the primary diagnostic aim and target population deviated from our specific latent variable and review scope. After identification, each record was marked as such and discussed with all three coders to determine whether the inclusion criteria were met. In consequence of the first instances, the inclusion criteria were more exclusively formulated concerning the diagnostic aim (operationalization as the latent variable cybersecurity SE) and target population (users). Coders were required to reach unanimous agreement on each subsequent borderline exclusion.

3.5 Coding Process

Three coders performed the study selection and data extraction. The reviewers were trained with $N = 10$ studies from 2009 (which were excluded a priori) each round until inter-rater agreement [87] reached a satisfactory level ($\iota > 0.6$). This was accomplished after the first round. Two iota coefficient indices were calculated using the R package irr [68] (R version: 4.0.3; package version: 0.84.1), one for nominal and one for continuous variables, whereby one key variable for each main query was accessed to determine the level of agreement for the training data sets: sample size, reliability alpha, as outcome variable, and intervention. The training yielded excellent agreement coefficients; for nominal data $\iota_{\text{training}} = 1$ and for interval data $\iota_{\text{training}} = 1$.

Prior to the sifts, study IDs were randomized using randomizer.org and and split into three blocks of about 232 publications each. Each reviewer was randomly assigned two of the three blocks, such that each study was coded twice. Moreover, we re-randomized all remaining studies after the full text sift, i.e., before data was extracted, and followed the same procedure as the first randomization (each reviewer coded a random two-thirds of included records). This ensured equal contributions and thus, acted as a countermeasure to potential biases caused by varying quantities of coding results by one of the reviewers. Reviewers were blinded to each other's decisions and in case of disagreements, they were discussed and decided by all three coders using a majority vote.

3.6 Data Evaluation

All coded study characteristics were defined in codebooks. Coders considered all sections of publications to evaluate data. For our coding scheme and a detailed description of each variable see the preregistration (OSF file link: codebook). The codebook included a-priori defined variables and value attributions to qualitative data or the specific format of extraction. Only a few variables were subject to open coding or paraphrasing (e.g., interventions or scale changes). Any additional steps for codes can be accessed in the coded data file (OSF file link: data; please see worksheet "additional steps" for further coding schemes). The subsections of the results section were a-priori determined based on the preregistered codes. Our reporting approach of the results is predominantly inductive (e.g., number of measures, referenced publications, practices regarding statistical tests, number of SE related variables, and intervention characteristics) with some deductive elements that were more theoretically informed (e.g., mapping of cause variables according to Bandura [21, 22]). We used a mixed-methods form of synthesis. For a qualitative approach to qualitative data, we relied on strategies

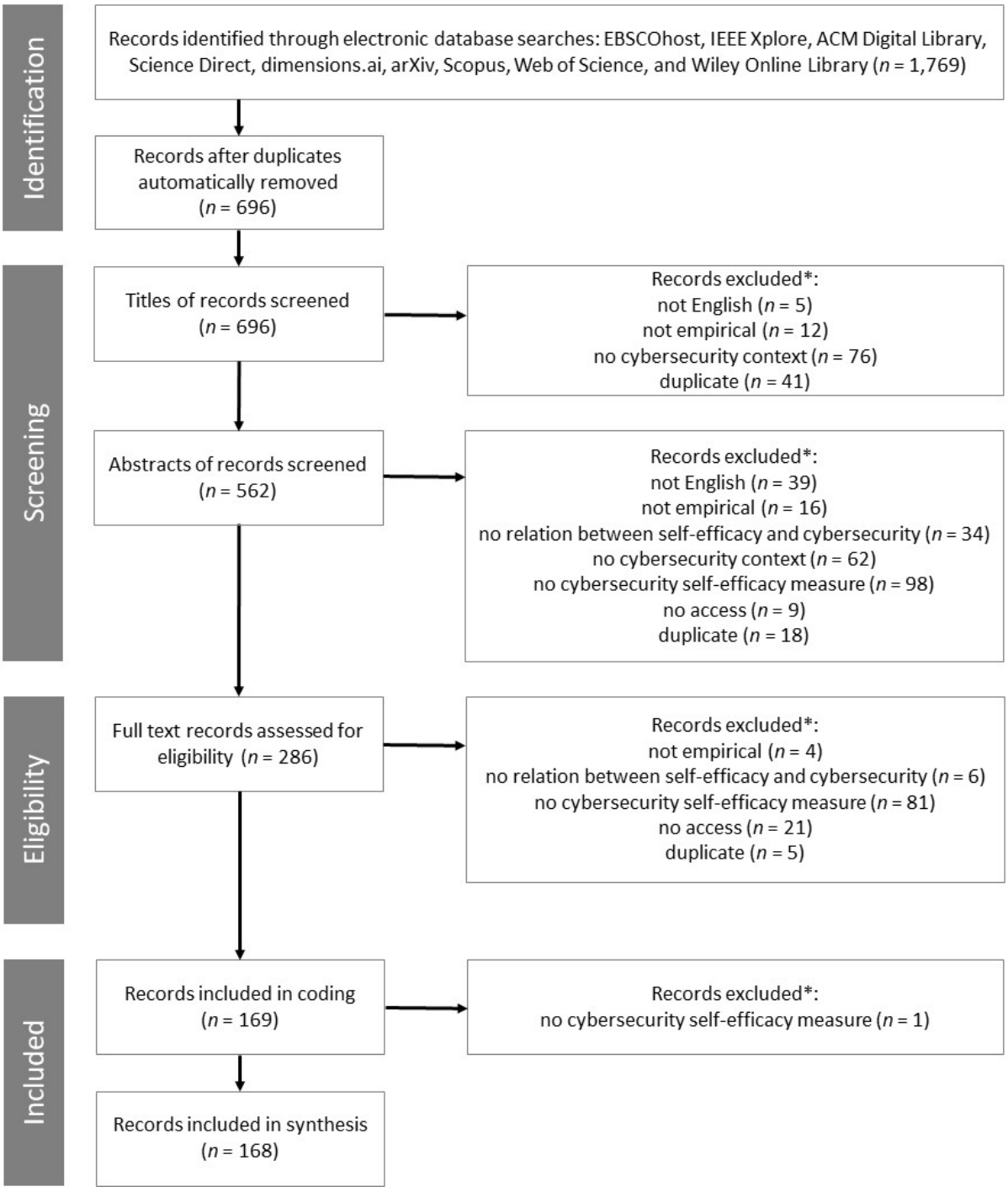


Figure 1: PRISMA Flow Diagram of Study Selection. Note. *Multiple reasons may apply.

from thematic synthesis (e.g., intervention types and methods) and framework synthesis (e.g., categorization of cause and outcome variables according to a-priori theories). For a quantitative approach to qualitative data, we incorporated content analyses (e.g., to quantify the occurrence of cause and outcome variables) and a network analysis (to compute the centrality of original scale authors). For a quantitative approach to quantitative data, we utilized numerical presentations (e.g., descriptive statistics of sample size or reliability coefficients). Variables were grouped into six categories: (a) publication information, (b) study information, (c) sample description,

(d) scale characteristics, (e) scale psychometrics, and (f) SE research model and intervention.

The first category concerning publication information surveyed the type, authors, year, title of the publication, and whether it was peer-reviewed. Additional title fields as well as the number of citations were also recorded. For study information, exclusion from synthesis, sample of multi-study papers, the type and setting of the study, and which technology the scale refers to were coded. Furthermore, we assessed the sample size, age and gender distribution, specific professions, country of origin, and recruitment strategy.

Scale characteristics involved variables for the origin of the scale, including its development, original authors, and changes made to the scale. We noted the scale's name and language, its number of items, factors, facets, and whether a definition for the construct was provided. If reported, we also extracted the wording of items. For all validation studies, we coded whether the definition fits the items and the type of item generation strategy. The category of scale psychometrics gathered information on different reliability coefficients and validity types. Both are central quality criteria for the eligibility of test instruments. While reliability is determined by the level of measurement errors, validity is assumed when a scale captures what it is intended to measure with sufficient accuracy [56]. Reliability variables were split to scope reported internal consistency (Cronbach's alpha and composite reliability), as well as test-retest and split-half reliability. For validity evidence, we looked at a) representative inference, which refers to the content validity of an instrument and the consultation of experts, b) theory-based interpretation, which refers to construct validity (including factor, discriminant, and convergent validity), and c) criterion-related inference, which involves both criterion validity with its three types (retrospective, competitive, and predictive validity) and incremental validity. Variables that reflected the research models were coded for measured cause and outcome constructs. We also recorded whether there was a use of interventions that were designed to explicitly influence self-efficacy or not and if applicable described the intervention and noted its replicability. In any cases of unreported data, authors were not contacted. Iota coefficient indices were calculated (as with training data) to assess the overall inter-rater agreement of our coding for multivariate observations using the R package irr [68] (R version: 4.1.3; package version: 0.84.1). We reached satisfactory values for both agreement coefficients; for nominal data $\iota_{\text{review}} = .722$ and for interval data $\iota_{\text{review}} = .982$

3.7 Risk of Bias

We minimized selection bias by defining clear selection criteria before data collection occurred, we covered a multitude of databases from different research disciplines, made sure to have a holistic and replicable search strategy, randomized studies for the selection process, had two blinded coders for each record, and catalogued the reasons for attrition. Still, inaccessible papers were dropped during the selection sifts. Language bias is plausible as we only included studies published in English. To limit publication bias effects, we incorporated grey literature search results. We used no study quality bias criteria because this review addresses methodological quality (e.g., reliability and validity) rather than substantive questions about the outcomes of the included studies.

4 RESULTS

All coded data and R scripts can be accessed and downloaded from OSF (OSF links: data and code) or GitHub repository (GitHub link removed for anonymization). First, the subsequent sections highlight results regarding scale characteristics, followed by psychometric data, and at last, SE models and interventions.

4.1 Current Measures of Cybersecurity Self-Efficacy

4.1.1 Heterogeneity of cybersecurity SE measures. Across 174 studies, we found 173 unique cybersecurity SE measures. A data set of all unique cybersecurity SE measures that includes publication information, scale name, referenced authors for item composition, and items are provided on the OSF: measures data set. Figure 2 visualizes the publication rate of measures in relation to studies for the review period under consideration. In this figure, no consolidation of measures after He et al.'s [76] review publication in 2014 can be observed. Of these 173 unique measures, only 5 were used more than once. No measure was used more than three times. Collapsing versions of measures (i.e., treating versions with minor word changes as the same) still yielded 155 cybersecurity SE measures (of which 9 were used more than once).

On average, scales consisted of $M_{n=150} = 5.41$ items ($SD = 6.03$, $MD = 4$, range = 1 to 54). We also assessed the latent variable structure via reported factors, i.e. structure based on mathematical information similarity between items, and facets, i.e. structure based on qualitative content similarity between items. Of the scales that featured a factor structure ($n = 13$), ten reported they consisted of one factor, two of 2, and one of 4. Where facets were reported ($n = 8$), they generally concerned specific security behaviors, types of threats, emotions, knowledge, or self-efficacy sources. Hence, authors often did not disclose the structure they assumed for SE, possibly treating SE as a single construct without explicit acknowledgment. We found a total of 8 measures that reported multiple sub-constructs, whether mathematical or qualitative. 133 measures offered specific definitions or explanations of the construct, which were not necessarily foundational to the scale development process. A comprehensive summary of the criteria reported with respect to the methodological rigor of the scales can be found in Table B1 and B2 in Appendix B.

The measures were often used without consistent specification of the technological context. We found, e.g., 136 publications involving non-specified technological contexts, 54 publications comprising computers, and 48 publications that involved general IT at workplaces. In contrast, only one publication studied smart home as a technological context (see supplementary materials for smart home results, file link: smart home results). The measures were published in 11 different languages, with English being the most common language at 57.23% and Chinese the second most common at 5.20%.

4.1.2 Citation network of cybersecurity SE measures. To identify potentially underlying similarities between scales, we investigated stated references (original authors) for item compositions with the help of a network analysis. Figure 3 shows the directed network graph of who cites who. The size of our author network was $N =$

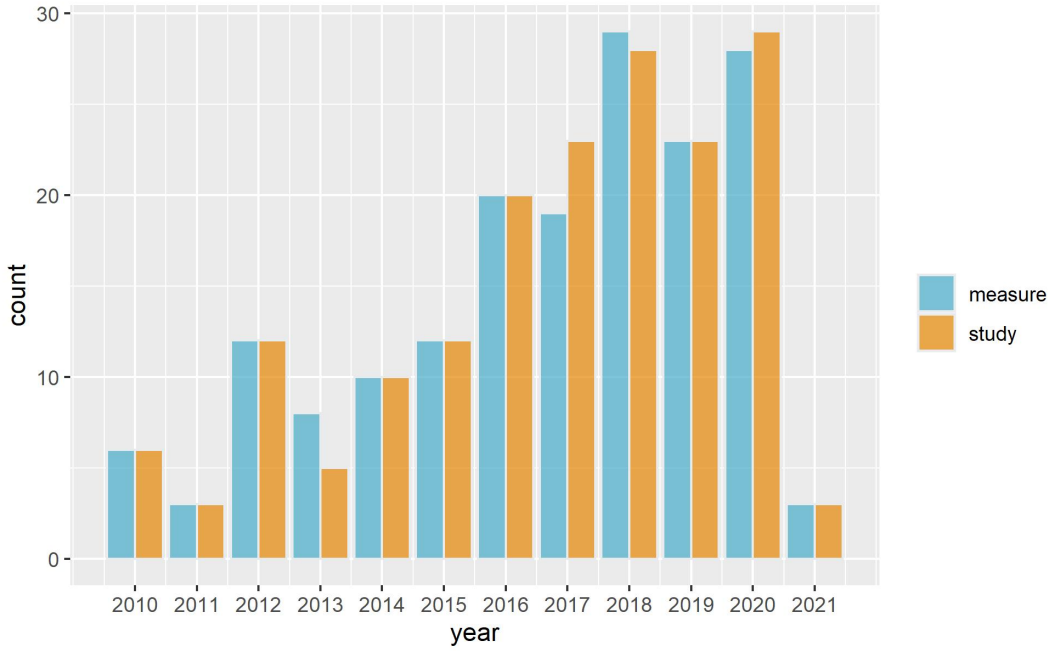


Figure 2: Histogram of Measure and Study Publication Rates

242, which equals the exact number of authors or author groups that were citing or were being cited.

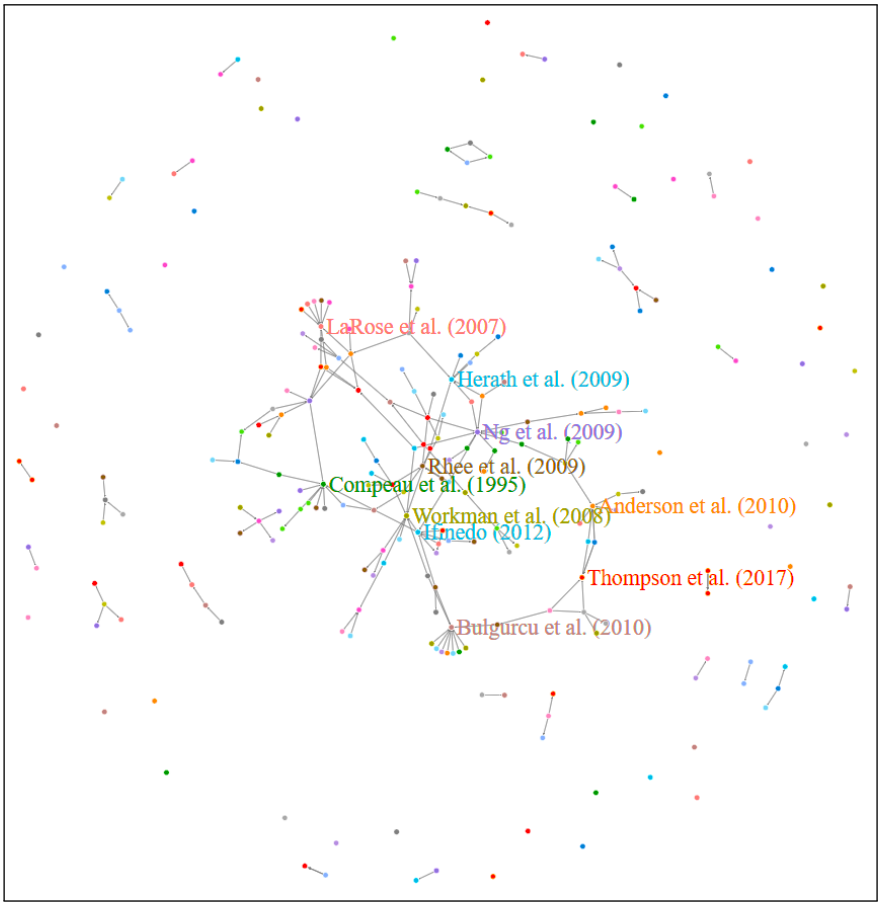
The most central nodes according to node strength (the sum of inward edge weights of a node) were both, Bulgurcu et al. [34] and Ng et al. [117], which were equally central with an InDegree centrality of IDC = 10. This centrality can be interpreted as the most referenced (10 citations each within this review) author groups as sources for item composition. An additional centrality measure for networks is betweenness (the frequency of a node in shortest paths between other nodes), indicating nodes that bridge information between fields and thus determining interdisciplinary used publications. With a betweenness centrality of BC = 18, Crossler [48] was the most central node.

To explore network clustering according to the small world principle (high clustering and low average path length), which is repeatedly found in natural graphs, we calculated the small world index. Our author network did not exhibit a small world structure, the index being SW = −2254.43. These results of the three centrality measures reveal very little underlying similarities, as we found neither an established common literature source for scale developments nor a network of references in which most scales are linked by only a few contiguous publications.

4.1.3 First use cybersecurity SE measures. First use measures, i.e., measures newly created or adapted for studies without being used before and without previous validity evidence, account for the overwhelming majority of cybersecurity SE assessments, making up 161 out of 173 measures. Readers seeking to further differentiate between newly created and adapted measures are encouraged to review our split analysis of key variables in Appendix C for more details. In the split analysis, we classified measures as newly created if they lacked reported original authors for their item compositions. Among the 161 measures, n = 118 (73.29%) were described as a modified version of a previous scale, n = 32 (19.88%) were developed as part of the empirical work, n = 2 (1.24%) were translations, and only n = 2 (1.24%) were equivalent to validating test developments. Another n = 7 (4.35%) did not report information on their development at all. Ad-hoc modifications, where reported, include changes to the wording (58 papers), number of items (11), translation (11), or general modifications (5). The two validation studies developed their items via deductive approaches and provided conceptual definitions of cybersecurity SE that were, in our understanding, not in full accordance with the respective operationalization.

4.1.4 Reliability of cybersecurity SE measures. Proceeding to the scales' psychometrics, Table 2 provides an overview of reported reliability information. Reliability estimates of first use scales indicated good coefficients when reported; weighted by sample size, mean coefficient alpha was $\alpha_{n=102} = .868$ ($SD = 0.062$) and composite reliability was $\text{CR}_{n=76} = .903$ ($SD = 0.055$) (unweighted $\alpha_{n=102} = .862$ ($SD = 0.073$) and $\text{CR}_{n=76} = .897$ ($SD = 0.058$)). Reliability analyses for split-half or test-retest reliability were not reported.

Scales with repeated use (recurring from prior publications $n_{\text{external}} = 12$ and recurring within review $n_{\text{internal}} = 5$), which we refer to as recurring scales, were similar to first use scales; mean coefficient alpha weighted by sample size was $\alpha_{n=10} = .871$ ($SD = 0.054$) (unweighted $\alpha_{n=10} = .877, SD = 0.077$) and the mean composite reliability weighted by sample size was $\text{CR}_{n=5} = .895$ ($SD = 0.055$) (unweighted $\text{CR}_{n=5} = .902, SD = 0.072$).



Legend

Authors	IDC
Anderson and Agarwal [17]	7
Bulgurcu et al. [34]	10
Compeau and Higgins [46]	9
Herath and Rao [78]	7
Ifinedo [85]	5
LaRose and Rifon [99]	8
Ng et al. [117]	10
Rhee et al. [129]	6
Thompson et al. [156]	5
Workman et al. [167]	8

Figure 3: Network Graph of Authors Developing Cybersecurity Self-Efficacy Measures. Note. The ten most referenced publications as sources for item composition within this review are labelled. Colors are specific to each reported (non-)reference. To identify the authors of each node, please use our interactive hmtl widget of the network provided on OSF (file link: authors network).

Table 2: Reliability Overview of Cybersecurity Self-Efficacy Measures

	Recurring	First Use
Number of measures	17[1]	161
Number of studies	18	156
Number of studies reporting reliability information[2]	11 (61.1%)	123 (78.8%)
Number of studies reporting...		
alpha coefficient	10 (55.6%)	102 (65.4%)
composite reliability	5 (27.8%)	76 (48.7%)
split-half reliability	–	–
test-retest reliability	–	–
Number of studies reporting...		
two out of four reliability estimates	4 (22.2%)	47 (30.1%)

Note. [1]Measures that were used more than once ($n = 5$) also count towards the first use measures column. The total number of measures is $N = 173$; [2]One study may report multiple reliability estimates.

4.1.5 Validity of cybersecurity SE measures. Validity information was reported by 10 studies with recurring scales (55.6%) and 117 studies with first use scales (75%). Table 3 provides an overview of reported validity types. As one strategy for content validity, 45 of 173 measures (26.01%) consulted experts to assess items. Exploring the factor structure of scales: 5 (3.11%) studies performed an EFA, 3 (1.86%) a CFA, 2 (1.24%) a PCA, and another 1 (0.62%) both, EFA and CFA. The types of analysis performed for discriminant validity split into: 5 (3.11%) correlations, 4 (2.48%) EFAs, 2 (1.24%) MTMMs, 2 (1.24%) CFAs, 2 (1.24%) AVEs, 81 (50.31%) other or mixed analyses, and 65 (40.37%) studies did not report any analysis. Regarding convergent validity statistical methods: 27 (16.77%) studies used the AVE, 6 (3.73%) a CFA, 5 (3.11%) an EFA, 2 (1.24%) a correlation, 53 (32.92%) other or mixed analyses, and the majority with 68 (42.24%) studies did not report any formal analysis. Criterion validity was analyzed with the help of Stone-Geisser Q-squared coefficients ($n = 1$).

To provide evidence for discriminant and convergent construct validity, studies drew on an immense variety of constructs. In total, 330 different constructs were used with the intention to validate cybersecurity SE scales. 13 constructs were used exclusively to discriminate from and another 19 exclusively to converge to cybersecurity SE. However, 298 were conceptualized as both discriminant and concurrently convergent across studies. The most frequent validation constructs in total counts were: perceived severity (88 models: 45 discriminant, 43 convergent), response efficacy (70 models: 36 discriminant, 34 convergent), perceived vulnerability (66 models: 33 discriminant, 33 convergent), response cost (32 models: 16 discriminant, 16 convergent), subjective norms (28 models: 14 discriminant, 14 convergent), and perceived susceptibility (22 models: 12 discriminant, 10 convergent).

4.2 Cybersecurity SE as Cause and Outcome

Evaluating research models, frames, and hypotheses, we found that 157 studies (90.23%) treated cybersecurity SE as a cause of another variable (such as security behavior), whereas 67 studies (38.51%) treated it as an outcome of other processes (e.g., awareness). Given that some research models conceptualized cybersecurity SE as a moderator, with an unclear causal positioning of self-efficacy, outcome variables of moderations were coded as outcomes of cybersecurity SE, even though the path diagram might have been more complex. We identified 173 unique outcome constructs (influenced by SE) and 103 cause constructs (influencing SE). Of these variables, 12 constructs were reported as both cause and outcome of SE across studies. We consolidated strongly related or nearly identical constructs with different spellings, e.g., (a) information computer security behavior and desktop security behavior were both synthesized as security behavior, (b) intention to comply with privacy policy and security compliance intention were both synthesized as compliance intention, or (c) awareness of information security policies and information security awareness were both synthesized as awareness. Two coders were tasked with identifying similarities in these variables, and when uncertain, they independently evaluated the underlying theoretical conceptualizations in the original publications. This process enhanced consistency across models and yielded 55 distinct outcome constructs, 51 cause constructs, and 19 outcome-and-cause constructs. Appendix D includes a list of these constructs and the frequency with which they were examined in studies. The most frequent outcome constructs were security behavior (25 studies), compliance intention (19 studies), and security intention (17 studies). For causes of cybersecurity SE, the most frequent variables were awareness (10 studies), expertise (7 studies), gender (7 studies). The most frequent outcome-and-cause constructs were awareness (13 studies), concerns (13 studies), and expertise (10 studies).

We further recoded these constructs to reflect originating theories or meta-levels of interest (see Figure 4). Since the reported theoretical perspective may be inconsistent within a publication (varying originating theories for definition, frameworks, empirical claims, and measures), we based our coding on measured variables. Coders inspected all sections from a publication to extract this information (including introduction, related work, or hypothesis sections). It is important to point out that our conclusions were not grounded in the reported results or the evidence level of variables; instead, our focus was on capturing the a-priori adopted theoretical assumptions.

Theories most prominently differ in the assumed proximity of cybersecurity SE to impact behavior, i.e., its direct or indirect effect through intention or motivation, and hence can serve to group outcome variables respectively. Here, behavior comprises both, observed and self-reported behaviors. Frequencies for outcome variables shown in Figure 4 reveal that no single theory seems to dominate the current literature on cybersecurity SE. However, motivation was not a process that was frequently hypothesized as an outcome, cf. Self-Determination Theory. Other outcome processes of cybersecurity SE included non-behavioral cognitive variables, such as concerns, awareness, or coping appraisal. The broad range of non-behavioral cognitive outcomes underline the diffuse role of cybersecurity SE in its nomological network as it is similarly posited by the Social Cognitive Theory.

Identified causal factors of cybersecurity SE were categorized to fit the four theoretically established sources of self-efficacy [cf. 21, 22]: mastery experience, (verbal) persuasion, emotional arousal, vicarious experience (see Figure 4). Much research on cybersecurity SE did not conform with this foundational taxonomy, and due to unclear theoretical rationales within included publications, the categorization was often unclear (50 out of 67 studies). Still, vicarious experience seems to be rather understudied in comparison to mastery experience and persuasion. The potential impact it's believed to have on cybersecurity SE could be utilized through approaches such as group interventions. Investigating this aspect with a focus on its scalability and effectiveness would be intriguing. Research interest in emotional arousal as a source of SE seems also limited, which could be attributed to its posited unreliable nature [21, 22]. Among the studied cause variables were other additional sources of self-efficacy that were of cognitive (33 incidences) and socio-demographic (14 incidences) nature (e.g., knowledge, awareness, or age). These additional cause variables can be taken as an opportunity to systematically study an expansion of theoretical assumptions of the Social Cognitive Theory. This also applies to reciprocal variables identified in this review. Bidirectional cause-and-effect pathways emerge as a relatively frequent phenomenon,

Table 3: Validity Overview of Cybersecurity Self-Efficacy Measures

	Recurring	First Use
Number of measures	17[1]	161
Number of studies	18	156
Number of studies reporting validity information[2]	10 (55.6%)	117 (75%)
Number of studies reporting...		
content validity	7 (38.9%)	86 (55.1%)
factor validity	2 (11.1%)	11 (7.1%)
discriminant validity	8 (44.4%)	96 (61.5%)
convergent validity	7 (38.9%)	93 (59.6%)
criterion validity	–	1 (0.6%)
incremental validity	–	–
Number of studies reporting...		
two out of six validity types	2 (11.1%)	31 (19.9%)
three out of six validity types	6 (33.3%)	56 (35.9%)
four out of six validity types	–	7 (4.5%)

Note. [1]Measures that were used more than once ($n = 5$) also count towards the first use measures column. The total number of measures is $N = 173$; [2]One study may report multiple validity types.

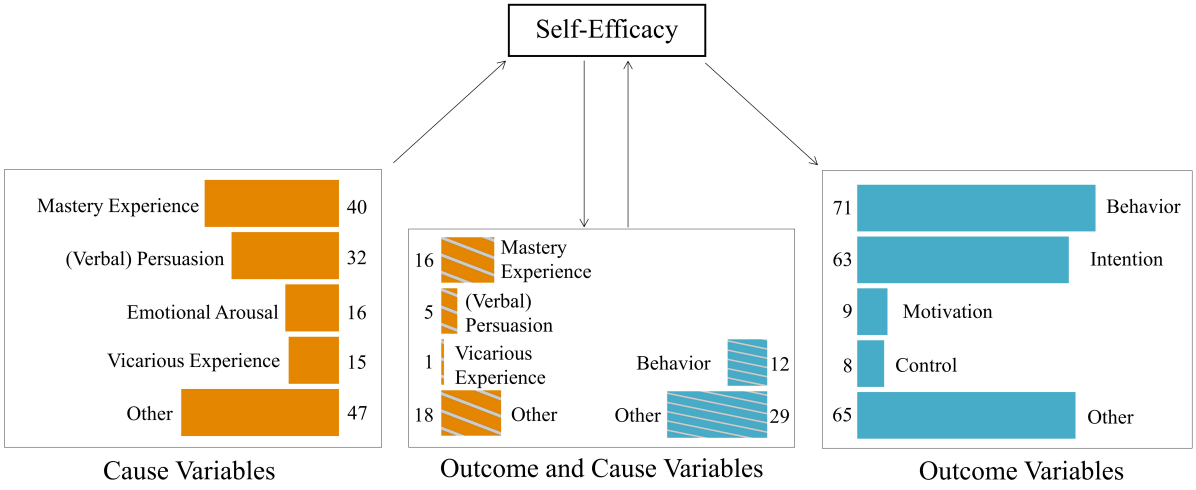


Figure 4: Synthesized Research Framework of Cybersecurity Self-Efficacy

demonstrating a diverse interpretation that has not yet been fully integrated into existing theory.

4.3 Current Interventions to Manipulate Cybersecurity SE

Only 13 out of 174 studies (7.47%) included a manipulation of cybersecurity SE (see Table 4). Generally, implemented interventions were designed to increase rather than decrease cybersecurity SE. These interventions included instructional components, learning materials, cybersecurity activities, and salience or awareness strategies. Interventions with activities consider mastery experience as a major source of self-efficacy in this review. However, this is our deduction as even in publications that included interventions, adherence to the foundational taxonomy provided by Bandura [21, 22] regarding the four SE sources was infrequently observed. Explanations of the underlying mechanisms by which specific intervention designs are expected to influence cybersecurity SE were also rarely provided. The interventions were evaluated by experimental or quasi-experimental designs with sample sizes ranging between $N = 19 - 442$ participants. Close to half of the interventions ($N = 6$) targeted students and interventions were primarily conducted with US American samples ($N = 11$). We found no replications of any intervention study. Regarding replicability, 2 out of 13 interventions [33, 169] provided the complete stimulus materials. Given that our focus is on reviewing research practices and methods, we did not further examine the findings or outcomes of the interventions and due to the scarcity of replication studies, we argue that the effectiveness of the identified interventions remains speculative.

Table 4: Cybersecurity Self-Efficacy Interventions

Authors	Intervention Type	Intervention Method	Study Type	Sample Size
Abraham [1]	training	instructional strategies of component display theory	experiment	151
Abraham and Chengalur-Smith [2]	training	instructional control elements	experiment	197
Amo [15]	training	cyber security related activity	quasi-experiment	34
Arachchilage [19]	game	cyber security related activity	quasi-experiment	20
Booth [33]	exposure to messages	cyber privacy risk awareness	experiment	201
Chen et al. [37]	game	cyber security related activity	experiment	178
Clark [43]	awareness campaign	compliance communication	quasi-experiment	246
He et al. [75]	training	text and video	experiment	119
Mamonov and Koufaris [110]	exposure to messages	government surveillance news	experiment	442
McGill et al. [112]	course	cyber security related activity and career awareness	quasi-experiment	19
Mwagwabi et al. [116]	training	fear appeals	experiment	210
Smith et al. [151]	training	in-house and third-party video	quasi-experiment	204
Zarouali et al. [169]	exposure to messages	privacy control salience	experiment	178

5 DISCUSSION

5.1 Implications for Cybersecurity SE Research

By assessing methodological practices of cybersecurity SE research conducted during the last decade, this systematic literature review provides meta-scientific evidence on heterogeneity, based on 168 publications concerning: (1) reported self-efficacy measures and their psychometric quality criteria, (2) the role of self-efficacy within its theoretical assumptions, and (3) implemented interventions designed to support cybersecurity self-efficacy. Regarding RQ1, we found 173 different cybersecurity SE measures, mostly used in just a single study. This implies that the issues of measurement inconsistency identified by He et al. [76] remain relevant, and have even intensified, given the increasing number of measures being published (see Figure 2). He et al. [76] also found scales that blend technology-focused items with more general ones, a practice that might lead to user confusion. This trend continues to be common [e.g., 10, 15, 40, 62, 94]. However, the research community has recently addressed dimensions of mobile and social media security [e.g., 5, 31, 54, 158], which were previously underrepresented, as highlighted by He et al. [76]. The scales show good reliability coefficients on average [for discussion on coefficient alpha and composite reliability see, 121], but critically neglected validity evidence. Unfortunately, most studies do not meet the guidelines available on how we ought to consolidate cybersecurity SE scales [76] and demonstrate validity [25, 27]. Although reliability is unquestionably important, it is validity evidence that grants meaningfulness to research findings. Systematically lacking validity evidence is a substantial threat to the usefulness of a research literature [57, 64]. Validated scales will improve resource allocation (time and effort invested in developing ad-hoc measures), research consistency (the ability to compare and combine data from studies on usable security), and quality control as the field converges on a measurement standard [105]. Otherwise, there is a risk of unreliable conclusions and an incoherent evidence base.

As there is no consensus on the operationalization of cybersecurity SE, the same is to be said for its theoretical understanding. He et al. [76] found that the definitions of SE are inconsistent among authors. Remarkably, these authors cited in He et al.'s [76] review are still frequently referenced for scale development [see Figure 3, references 85, 117, 129]. This suggests that different theoretical assumptions continue to be a fundamental aspect in the field. Nonetheless, we found that (a) a vast majority of publications provided definitions or construct clarifications, and (b) in several instances specific scale names were differentiated according to the context of SE [e.g., 31, 41, 49, 171], as suggested by He et al. [76]. As for RQ2, we observed a critical quantity of distinguishable frameworks, amounting to at least 55 outcome, 51 cause, and 19 outcome-and-cause variables of cybersecurity SE. References to self-efficacy theories are particularly evident for outcomes, with no theory clearly dominating the literature. He et al.'s [76] findings already hinted at the prominent role of SE in influencing a variety of dependent variables. Regarding the sources of self-efficacy, the literature has a limited fit with established frameworks, but we found two additional important research foci of causes of cybersecurity SE: cognitive and socio-demographic variables. This general scarcity of reporting specific and consistent theoretical underpinnings is also salient in other self-report measures published in HCI outlets [6]. As the field advances, achieving a unified understanding of the literature should be an important objective [60].

This fragmented picture persists for RQ3, which addresses cybersecurity SE interventions. Not one of the 13 studies with interventions was replicated. Conclusions about the general effectiveness of the interventions' methods are therefore speculative at best. Interventions rarely derived their methods explicitly from theoretically established SE sources; still, several interventions relied on cybersecurity activities implying the relevance of mastery experience. These findings extent He et al.'s [76] observations about confusion surrounding the impact of SE. We advocate not to neglect practical implications that can be carefully deducted from SE theory and dismiss the opportunity to provide detailed reasoning for specific decisions about intervention methods. Alternatively, researchers are limited in their exploration of methodological evidence and it remains uncertain, also to any practitioner interested in implementing SE interventions, how robust effect mechanisms are that influence security behaviors [cf. 122]. An unclear onus of proof may

reduce trust in the intervention's capacity to resolve the underlying issue. It may be that authors shy away from replications because (a) original studies lack detailed information, (b) translation processes might be necessary as the field is rather diverse (30 countries in this review alone), and (c) replications are much harder to publish than original works [cf. 84, 131].

5.2 Recommendations

Researchers draw on a wide range of measures and interventions, though this decision is not consistently based on best performing quality criteria, which further emphasises the need for cybersecurity SE validation and replication research. Valid conclusions about genuine effects and effective interventions to increase cybersecurity SE are only possible to the degree of the primary studies' quality level [106, 131]. Which leads us to the following three recommendation sections based on our research questions: (1) measures, (2) theoretical assumptions, and (3) interventions.

5.2.1 Measures. Transparency of measures should be habituated by always providing a scale manual in the supplementary material section of a publication. Manuals need to include at least instructions, items, their origin, response scale, and scoring strategies. We recommend including thorough assessments of psychometric quality criteria as well [cf. 51]. Researchers seeking to create transparent manuals may find Aeschbach et al.'s [6] prescriptive model for the measurement selection process beneficial. This increases the scales' reusability, warrants criteria based decision-making when or how to include an instrument, and allows access to necessary information for reproducibility and replicability. For notable examples of transparent reporting and consistent measure usage, we recommend the User Experience Questionnaire (UEQ) [100, 143] or Raven's Progressive Matrices (RPM) [127, 166] to readers. Although this might appear trivial, it was our experience that the current state of reporting did not allow us to, e.g., differentiate indisputably between newly created and adapted measures. Publications may cite another, original paper and thus be categorized as using an adapted measure, but (a) make substantial changes to domain, item wording, or number of items [e.g., 30, 97, 148], (b) cite multiple original authors [e.g., 40, 85, 136], which could as well indicate a common and even recommended strategy in literature to construct new scales, or (c) report no items [e.g., 4, 14, 32], making the level of adaption or novelty ambiguous to the reader. Other publications may not report original authors [e.g., 69, 73, 92]. To optimize transparency, we suggest even including an item-level change log in the manual.

We also urge researchers to not modify or develop scales within the same empirical work from which it draws substantive inferences. When researchers find it necessary to change existing measures or create new ones, they should first conduct a study to evaluate the psychometric quality of these measures [58]. Subsequently, a separate study should be undertaken using a new sample to investigate the relevant research question with the then-validated measures. In other words, mingling the interpretation of a substantive effect on a variable (e.g., whether an intervention increases SE) and the suitability of its operationalization (e.g., whether a scale actually measures SE) within the same study ought to be avoided. Best practices and guidance for scale construction processes are widely available [e.g., 25, 67, 115, 142]. A concerted dedication of the research community's effort and time in constructing a reliable and valid cybersecurity SE scale, will facilitate its impact and applications. In an attempt to reduce measure heterogeneity, an exemplary scale that one could build upon if construct specificity and contemporary security issues were to be addressed is the Self-Efficacy in Information Security scale by Rhee et al. [129]. We further recommend that those preceding validation studies adopt a more advanced psychometric perspective, specifically item response theory (IRT), which encompasses more appropriate measurement models for more detailed evaluations of item qualities [cf. 67]. For instance, IRT allows researchers to examine option characteristic curves for each item, as well as item or test information functions (see Choi and Asilkalkan [39] for a helpful guide).

5.2.2 Theoretical assumptions. Measurement standards will then set the foundation for theory and model comparisons (and elimination, cf. 138, 139). Based on our understanding of scientific progress, we strongly recommend striving for parsimony and falsification of SE theories across scientific disciplines. An original theory of self-efficacy that otherwise meets the criteria of theory evaluation, such as consistency and testability [63], should be first trialed for its adequacy. Our experience showed that the varied interpretations of SE's role stem not only from differing theoretical assumptions but also, more significantly, from deviations from the respective original theory (see the extent of the categories labelled "other" in Figure 4). However, the proposition of new and more complex models is only reasonable when it significantly enriches the theory's explainability and should always be comprehensively justified. The results presented in Figure 4 might though imply such a reasonable revision, suggesting a diverse understanding of both outcome and cause variables, potentially considering them as reciprocal.

In particular, we caution against mixed theory referencing across the introduction of the SE construct and its measurement. Citing, e.g., Bandura's works [21, 22] or related sources for the definition of SE, and then applying SE scales based on users' perceived cybersecurity knowledge [see 73, 165], can cause ambiguity. This is due to Bandura's [24] objection to conflating knowledge with self-efficacy. An unclear or divided theoretical understanding can jeopardize cross-disciplinary collaborations due to the lack of a common language (while expertise from multiple disciplines is required for many HCI research questions) and the field's scientific progress by delaying the discovery of relevant patterns (given that solid foundations are critical for valid research designs) [125]. Hence, we recommend the following: (a) consistently adhere to an adequately tested theory and revise with prudence across publications; (b) maintain the assumptions of that framework within each publication; and (c) apply this consistency to both cause and outcome variables of SE as well. The consequences of not following the latter point are evident in the heterogeneity of the terminologies found in our results, although the full extent is uncertain due to potential redundancy. For researchers interested in illustrating commonalities among psychological constructs, we would like to refer to Hodson [80]. We specifically encourage authors to contribute to

such more robust categories, i.e. to minimize the "other" categories as presented in Figure 4.

5.2.3 Interventions. In contrast to the substantial amount of measures and related constructs, we discovered only a limited number of interventions designed to support cybersecurity SE. We recommend that more theory-driven paradigms for interventions should be developed. Based on our observations, presumed pathways for influencing cybersecurity SE were rarely reported explicitly. Researchers or practitioners interested in the development of conceptually grounded interventions might find publications by Bandura [21, 23, 24] in combination with the introductory book by Cooper et al. [47] a useful foundation. As a proposition for future work, we suggest to evaluate newly designed interventions regarding: (a) the level and sustainability of effectiveness, (b) its generality across specific samples and situations, and (c) economic application factors, e.g. through the dose-response relationship [cf. 74]. It will be decisive to see whether interventions affect individuals uniformly or whether they interact with specific personological or situational factors.

In order to obtain robust empirical evidence from these interventions, we recommend replicating the interventions. None of the currently published interventions (see Table 4) has been replicated. The call for replication research is imperative as other large-scale replication projects have demonstrated the uncertainty of original empirical evidence in the social sciences [119]. To which extent the same is true for cybersecurity SE research is difficult to estimate given the current research practices in this domain. Overall, the HCI community has made progress in transparent reporting for better replicability. However, the sharing of data and artifacts, essential for replicating interventions, is still relatively limited [137]. In our review, only 2 out of 13 interventions offered complete stimulus materials. Even if authors may feel confident about replicability based on the information they provide [159], we suggest that both authors and reviewers adopt reporting screening systems, such as proposed by Salehzadeh Niksirat et al. [137], to increase access to intervention materials. In other words, we recommend transparency for designed manipulations by sharing all instructions and materials involved [see 81]. This can be achieved via permanent links to public repositories, e.g., OSF.io or PsychArchives.org.

We find that our recommendations might extend beyond the realm of cybersecurity SE research and are also relevant to a broader issue encountered in various disciplines involving psychological measures [cf. 58]. However, the context of IT security and privacy is of imminent relevance due to the increasing state of data proliferation, which includes sensitive information that can have a significant personal and economic impact when exploited. As cybersecurity is also a multidisciplinary field, it encounters a distinct set of challenges not necessarily found in all scientific disciplines. Some disciplines, such as cognitive performance or personality research, have more established and homogeneous methodological approaches, where our recommendations might not find as well-suited an environment [61, 89, 98].

This systematic review was crucial for substantiating our recommendations empirically. While one could also consider replications of specific studies for empirical evidence also concerning robustness, our primary objective was to evaluate the overall extent of heterogeneity in the cybersecurity SE literature across publications. Prior to this review, it was unclear whether researchers' current understanding of the relevance of methodological consistency would render our recommendations unfit. Yet, our review provides empirical data for the indispensability of our recommendations: whether it is to (a) encourage a shift towards greater transparency and replicability in methodological practices and reporting standards in research or (b) raise the public's awareness of the validity (or lack thereof) of existing recommendations for motivating security behavior.

5.3 Limitations

There are two important types of limitations inherent in this literature review: (a) limitations of evidence and inferences, and (b) limitations of review methods. The former is mainly shaped by the simple difference between reporting standards (or more likely reporting constraints, such as limited word counts for publications) and performed back-end research processes. This limits the possible inferences made with regard to the current heterogeneity of the literature, two of which we would highlight exemplarily: First, more detailed information on scales (e.g., a standard reporting of items) might have lead to a different estimate of the number of (unique) cybersecurity SE measures in use. Second, structured reporting of the scale development process might have revealed more commonalities between scales. Beyond missing information, the measurement heterogeneity would be smaller if on an empirical level, cybersecurity SE measures were to measure the same individual manifestation (mean cybersecurity SE scores) across differently constructed scales. The consequences of using different measures could thus be mitigated if scores would be identical, proving that no jingle fallacy occurred.

Similar arguments can be made with regard to the large number of cybersecurity SE cause/outcome constructs. Similar operationalizations of some of these would imply redundant constructs (see also "jangle fallacy", cf. 80), and hence, the picture of cybersecurity SE's role within frameworks would be more consistent than it might appear. The prominence of theories might also be more evident if publications consistently referred to one perspective throughout, but this was not observed. Therefore, we concentrated on hypothesized causality, often depicted as measurement models, which did not always align with any specific theory. One also might consider the possibility that though constructs were formulated and measured as behavioral intentions, authors were in fact hypothesizing direct effects on behavior but did not have the resources or opportunity to implement a behavioral measure. All four aspects could be causes for false dividedness across publications.

Other limitations concern the quality of reported scale validation techniques. There were profound differences in quality of the performed studies which were not highlighted in our review. In particular, we found that the methods used for construct validity did not consistently reflect an understanding of the purpose of demonstrating the convergent and discriminant validity. As for interventions to foster cybersecurity SE, the theoretical mechanisms were in most cases merely implicitly retraceable (e.g., the connection between implemented cybersecurity activities and mastery

experience, see, 21), and often not explicitly justified. Other interventions in this review incidentally showed an intervention effect on cybersecurity SE; however, those were not explicitly designed to affect cybersecurity SE, and were not included as cybersecurity SE interventions due to their lack of a theoretical rationale.

Limitations of review methods involve the date of data collection, search strategies, and the coding process. Data collection occurred in March 2021, excluding more recent publications in the field. Periodically updating this review will eventually enable a trend analysis of the methods used. This is a call to future work as we find it valuable to consolidate practices and their pattern of progression. Updating is also of great importance when reviews synthesize meta-analytic evidence on substantive research questions about the outcome of studies (e.g., does cybersecurity SE predict security behaviors), where omitting new studies is a relevant issue. The objective of this review was to assess the heterogeneity of research practices (see goal 1-3), and these findings remain valid as (a) they reflect the respective understanding of the subject matter and (b) continue to be relevant for even the latest publication in the field, which still reveal non-adoption of methodological standardization [such as, 36, 38, 44, 52, 53, 86, 91, 95, 101, 102, 104, 114, 145, 147, 157].

Additionally, biases could result from search terms we may have missed (e.g., names of brand specific IT devices) or unpublished studies remaining undiscovered in the file drawer. If those works were to more homogeneously rely on similar measures and theory principles, they would shift our review findings towards a more unified cybersecurity SE literature respectively. And at last, though the inter-rater agreement coefficient for nominal data is satisfactory, there were some differences in coding, ultimately resolved by group discussion, when there was too much room for interpretation in the research.

5.4 Conclusion

This systematic literature review paints a fragmented picture of current cybersecurity SE research methods. Over the past decade, studies on SE and IT security have revealed limited use of standardized measurement, model, and intervention methods, which can constrain our ability to draw meaningful conclusions on the subject. We identified 168 relevant publications for synthesis including 173 cybersecurity SE measures. Most indicated good reliability coefficients, however missed essential validity analyses. There were 173 outcome as well as 103 cause variables, some having ambiguous causal links, and some being conceptualized as both outcome and cause of cybersecurity SE. Of 13 intervention studies to improve cybersecurity SE, none was replicated. The lack of consensus might be rooted in the current state of self-efficacy theories that prevail side by side, resulting in deviating methods. The field's multi-disciplinary nature may be another important context factor, as each field may focus on a different aim than the replicability of findings beyond their discipline. We propose steps that we hope will encourage a shift towards greater consistency in cybersecurity SE methods. These recommendations will enable researchers to more clearly assess the extent to which the presumed relevance of self-efficacy for security behaviors mirrors today's strong visibility of cybersecurity SE research and will provide practitioners with effective material to impact modern IT security and privacy.

ACKNOWLEDGMENTS

This research was supported by the German Federal Ministry of Education and Research (BMBF, grant no. 16SV8505), the German Research Foundation (DFG) under Germany's Excellence Strategy (grant no. EXC 2092 CASA - 390781972), and the META-REP Priority Program of the German Research Foundation (DFG, grant no. 464488178).

REFERENCES

[1] Sherly Abraham. 2012. *Exploring the effectiveness of information security training and persuasive messages: Dissertation.* ProQuest LLC, Ann Arbor, MI, USA.

[2] Sherly Abraham and InduShobha Chengalur-Smith. 2019. Evaluating the effectiveness of learner controlled information security training. *Computers & Security* 87 (2019), 101586. https://doi.org/10.1016/j.cose.2019.101586

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2018. Nudges for privacy and security. *Comput. Surveys* 50, 3 (2018), 1–41. https://doi.org/10.1145/3054926

[4] John Agyekum Addae, Grace Simpson, and George Oppong Appiagyei Ampong. 2019. Factors Influencing Information Security Policy Compliance Behavior. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT).* IEEE, Accra, Ghana, 43–47. https://doi.org/10.1109/ICSIoT47925.2019.00015

[5] Kishalay Adhikari and Rajeev Kumar Panda. 2018. Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing* 31, 2 (2018), 1–15. https://doi.org/10.1080/08911762.2017.1412552

[6] Lena Fanya Aeschbach, Sebastian A.C. Perrig, Lorena Weder, Klaus Opwis, and Florian Brühlmann. 2021. Transparency in Measurement Reporting. *Proceedings of the ACM on Human-Computer Interaction* 5, CHI PLAY (2021), 1–21. https://doi.org/10.1145/3474660

[7] Icek Ajzen. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (1991), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

[8] Blessing Akinrotimi. 2023. Systematic review of cybersecurity pedagogical tools: Master Thesis. https://www.proquest.com/openview/f610ae2952cdc715c886f643701ed8cb/1?pq-origsite=gscholar&cbl=18750&diss=y

[9] Maryam Nasser AL-Nuaimi. 2022. Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review: ahead-of-print. *Global Knowledge, Memory and Communication* ahead-of-print, ahead-of-print (2022), ahead–of–print. https://doi.org/10.1108/GKMC-12-2021-0209

[10] Sultan T. Alanazi, Mohammed Anbar, Shouki A. Ebad, Shankar Karuppayah, and Hadeer A. Al-Ani. 2020. Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry* 12, 9 (2020), 1544. https://doi.org/10.3390/sym12091544

[11] Afrah Almansoori, Mostafa Al-Emran, and Khaled Shaalan. 2023. Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences* 13, 9 (2023), 5700. https://doi.org/10.3390/app13095700

[12] Abdulelah Alshammari, Vladlena Benson, and Luciano C. Batista. 2023. Emotional Cost of Cyber Crime and Cybersecurity Protection Motivation Behaviour: A Systematic Literature Review. In *PACIS 2023 Proceedings.* AIS, Nanchang, China, 133. https://aisel.aisnet.org/pacis2023/133

[13] Rawan A. Alsharida, Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society* 73 (2023), 102258. https://doi.org/10.1016/j.techsoc.2023.102258

[14] Yazan Alshboul and Kevin Streff. 2017. Beyond Cybersecurity Awareness. In *Proceedings of the 2017 International Conference on Software and e-Business.* ACM, New York, NY, USA, 85–91. https://doi.org/10.1145/3178212.3178218

[15] Laura Amo. 2016. Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy. *IEEE Security & Privacy* 14, 1 (2016), 72–75. https://doi.org/10.1109/MSP.2016.12

[16] Laura Amo, Ruochen Liao, Emma Frank, H. Raghav Rao, and Shambhu Upadhyaya. 2019. Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education* 62, 2 (2019), 134–140.

[17] Catherine L. Anderson and Ritu Agarwal. 2010. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly* 34, 3 (2010), 613–643. https://doi.org/10.2307/25750694

[18] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69, 4 (2017), 437–443. https://doi.org/10.1016/j.chb.2016.12.040

[19] Nalin A. G. Arachchilage. 2016. *Serious Games for Cyber Security Education*. LAP Lambert Academic Publishing, London, UK.

[20] Kregg Aytes and Terry Conolly. 2003. A Research Model for Investigating Human Behavior Related to Computer Security. In *AMCIS 2003 Proceedings*, Association for Information Systems (Ed.). AIS Electronic Library, Tampa, FL, USA, 2027–2031. https://aisel.aisnet.org/amcis2003/260

[21] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84, 2 (1977), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

[22] Albert Bandura. 1986. *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall, Englewood Cliffs, NJ, USA.

[23] Albert Bandura. 1997. *Self-efficacy: The exercise of control*. W H Freeman/Times Books/ Henry Holt & Co, New York, NY, USA.

[24] Albert Bandura. 2004. Health promotion by social cognitive means. *Health Education & Behavior* 31, 2 (2004), 143–164. https://doi.org/10.1177/1090198104263660

[25] Albert Bandura. 2006. Guide for constructing self-efficacy scales. In *Self-efficacy beliefs of adolescents*, Frank Pajares and Timothy C. Urdan (Eds.). IAP - Information Age Pub. Inc, Greenwich, CT, USA, 307–337.

[26] Albert Bandura. 2010. Self-Efficacy. In *The Corsini Encyclopedia of Psychology*, Irving B. Weiner and W. Edward Craighead (Eds.). John Wiley & Sons, Inc, Hoboken, NJ, USA. https://doi.org/10.1002/9780470479216.corpsy0836

[27] Albert Bandura. 2012. On the Functional Properties of Perceived Self-Efficacy Revisited. *Journal of Management* 38, 1 (2012), 9–44. https://doi.org/10.1177/0149206311410606

[28] Masooda Bashir, Colin Wee, Nasir Memon, and Boyi Guo. 2017. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security* 65 (2017), 153–165. https://doi.org/10.1016/j.cose.2016.10.007

[29] Adam Beautement and Angela Sasse. 2009. The economics of user effort in information security. *Computer Fraud & Security* 2009, 10 (2009), 8–12. https://doi.org/10.1016/S1361-3723(09)70127-7

[30] France Belanger and Robert E. Crossler. 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems* 28, 1 (2019), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

[31] Ardion Beldad. 2016. Sealing One's Online Wall Off From Outsiders: Determinants of the Use of Facebook's Privacy Settings among Young Dutch Users. *International Journal of Technology and Human Interaction* 12, 1 (2016), 21–34. https://doi.org/10.4018/ijthi.2016010102

[32] Jean-Francois Berthevas. 2018. Students' computers safety behaviors, under effects of cognition and socialization: When gender and job experience influence information security behaviors. In *2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*. IEEE, Piscataway, NJ, USA, 244–251.

[33] Cheryl Lynn Booth. 2019. *Tipping the balance in privacy calculus: The roles of perceived trustworthiness, uncertainty, and cyber self-efficacy in an online user's intention to disclose PII*. Ph. D. Dissertation. Florida State University, Tallahassee, FL, USA.

[34] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34, 3 (2010), 523–548. https://doi.org/10.2307/25750690

[35] Mark Chan, Irene Woon, and Atreyi Kankanhalli. 2005. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security* 1, 3 (2005), 18–41. https://doi.org/10.1080/15536548.2005.10855772

[36] Hsin Hsin Chang, Kit Hong Wong, and Ho Chin Lee. 2022. Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. *Electronic Commerce Research and Applications* 54 (2022), 101176. https://doi.org/10.1016/j.elerap.2022.101176

[37] Tianying Chen, Margot Stewart, Zhiyu Bai, Eileen Chen, Laura Dabbish, and Jessica Hammer. 2020. Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference (DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1737–1749. https://doi.org/10.1145/3357236.3395522

[38] Hichang Cho. 2023. Heterogeneous User Responses to Privacy Risks in Mobile Apps: Understanding the Dualistic Role of Privacy Risk Perceptions. In *Proceedings of the 25th International Conference on Mobile Human-Computer Interaction*, Andreas Komninos, Carmen Santoro, Damianos Gavalas, Johannes Schoening, Maristella Matera, and Luis A. Leiva (Eds.). ACM, New York, NY, USA, 1–7. https://doi.org/10.1145/3565066.3608694

[39] Youn-Jeng Choi and Abdullah Asilkalkan. 2019. R Packages for Item Response Theory Analysis: Descriptions and Features. *Measurement: Interdisciplinary Research and Perspectives* 17, 3 (2019), 168–175. https://doi.org/10.1080/15366367.2019.1586404

[40] Hui-Lien Chou and Chien Chou. 2016. An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior* 65 (2016), 334–345. https://doi.org/10.1016/j.chb.2016.08.034

[41] Hui-Lien Chou and Jerry Chih-Yuan Sun. 2017. The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education* 112 (2017), 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

[42] Noman H. Chowdhury, Marc T. P. Adam, and Geoffrey Skinner. 2019. The impact of time pressure on cybersecurity behaviour: a systematic literature review. *Behaviour & Information Technology* 38, 12 (2019), 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769

[43] Christine Y. Clark. 2013. *A study on corporate security awareness and compliance behavior intent: Dissertation*. ProQuest LLC, Ann Arbor, MI, USA.

[44] Julien Cloarec. 2022. Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. *Journal of Business Research* 152 (2022), 144–153. https://doi.org/10.1016/j.jbusres.2022.07.045

[45] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David Weintrop. 2020. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming* 51, 5 (2020), 586–611. https://doi.org/10.1177/1046878120933312

[46] Deborah R. Compeau and Christopher A. Higgins. 1995. Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research* 6, 2 (1995), 118–143. https://doi.org/10.1287/isre.6.2.118

[47] John O. Cooper, Timothy E. Heron, and William L. Heward. 2019. *Applied Behavior Analysis* (third edition ed.). Pearson, Hoboken, NJ.

[48] Robert E. Crossler. 2010. Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. In *43rd Hawaii International Conference on System Sciences (Hicss)*. IEEE, Honolulu, HI, USA, 1–10. https://doi.org/10.1109/HICSS.2010.311

[49] Robert K. Day. 2018. *Modeling the influence of personal characteristics on information security policy compliance in US-based financial, medical, and information services industries*. Vol. 79. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2018-26094-231&site=ehost-live

[50] Edward L. Deci and Richard M. Ryan (Eds.). 2002. *Handbook of self-determination research*. University of Rochester Press, Rochester, NY, USA.

[51] Diagnostik- und Testkuratorium. 2018. TBS-DTK. Testbeurteilungssystem des Diagnostik- und Testkuratoriums der Föderation Deutscher Psychologenvereinigungen: Revidierte Fassung vom 03. Jan. 2018. *Psychologische Rundschau* 69, 2 (2018), 109–116. https://doi.org/10.1026/0033-3042/a000401

[52] Cassandra E. Dodge, Nathan Fisk, George W. Burruss, Richard K. Moule, and Chae M. Jaynes. 2023. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy* 22, 4 (2023), 849–868. https://doi.org/10.1111/1745-9133.12641

[53] Ahmet Duzenci, Hakan Kitapci, and Mehmet Sahin Gok. 2023. The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences* 13, 15 (2023), 8731. https://doi.org/10.3390/app13158731

[54] Esther Dzidzah, Kwame Owusu Kwateng, and Benjamin Kofi Asante. 2020. Security behaviour of mobile financial service users. *Information and Computer Security* 28, 5 (2020), 719–741. https://doi.org/10.1108/ics-02-2020-0021

[55] Matthew S. Eastin and Robert LaRose. 2000. Internet Self-Efficacy and the Psychology of the Digital Divide. *Journal of Computer-Mediated Communication* 6, 1 (2000), JCMC611. https://doi.org/10.1111/j.1083-6101.2000.tb00110.x

[56] Michael Eid and Katharina Schmidt. 2014. *Testtheorie und Testkonstruktion*. Hogrefe, Göttingen, Germany. http://sub-hh.ciando.com/book/?bok_id=1548490

[57] Malte Elson. 2019. Examining Psychological Science Through Systematic Meta-Method Analysis: A Call for Research. *Advances in Methods and Practices in Psychological Science* 2, 4 (2019), 350–363. https://doi.org/10.1177/2515245919863296

[58] Malte Elson, Ian Hussey, Taym Alsalti, and Ruben C. Arslan. 2023. Psychological measures aren't toothbrushes. *Communications Psychology* 1, 1 (2023), 25. https://doi.org/10.1038/s44271-023-00026-9

[59] ENISA. 2019. Cybersecurity culture guidelines: Behavioural aspects of cybersecurity: European Union Agency For Network and Information Security Report 2019. https://doi.org/10.2824/324042

[60] Robert Epstein. 1984. The Principle of Parsimony and Some Applications in Psychology. *The Journal of Mind and Behavior* 5, 2 (1984), 119–130.

[61] Arne Evers, José Muñiz, Dave Bartram, Dusica Boben, Jens Egeland, José R. Fernández-Hermida, Örjan Frans, Grazina Gintilienė, Carmen Hagemeister, Peter Halama, Dragos Iliescu, Aleksandra Jaworowska, Paul Jiménez, Marina Manthouli, Krunoslav Matesic, Mark Schittekatte, H. Canan Sümer, and Tomáš Urbánek. 2012. Testing Practices in the 21st Century. *European Psychologist* 17, 4 (2012), 300–319. https://doi.org/10.1027/1016-9040/a000102

[62] Chidi Ezuma-Ngwu. 2019. *Exploring individual intent towards blockchain technology in response to threats to personal data and privacy*. Vol. 81. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-31102-001&site=ehost-live

[63] Jacqueline Fawcett. 2005. Criteria for evaluation of theory. *Nursing Science Quarterly* 18, 2 (2005), 131–135. https://doi.org/10.1177/0894318405274823

[64] Jessica Kay Flake, Ian J. Davidson, Octavia Wong, and Jolynn Pek. 2022. Construct validity and the validity of replication studies: A systematic review. *The American psychologist* 77, 4 (2022), 576–588. https://doi.org/10.1037/amp0001006

[65] Jessica Kay Flake and Eiko I. Fried. 2020. Measurement Schmeasurement: Questionable Measurement Practices and How to Avoid Them. *Advances in Methods and Practices in Psychological Science* 3, 4 (2020), 456–465. https://doi.org/10.1177/2515245920952393

[66] Anja Frei, Anna Svarin, Claudia Steurer-Stey, and Milo A. Puhan. 2009. Self-efficacy instruments for patients with chronic diseases suffer from methodological limitations–a systematic review. *Health and Quality of Life Outcomes* 7 (2009), 86. https://doi.org/10.1186/1477-7525-7-86

[67] Mike Furr. 2011. *Scale Construction and Psychometrics for Social and Personality Psychology*. SAGE Publications, London, UK. http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10719206

[68] Matthias Gamer, Jim Lemon, Ian Fellows, and Puspendra Singh. 2019. Various Coefficients of Interrater Reliability and Agreemen: Package 'irr'. https://cran.r-project.org/web/packages/irr/irr.pdf

[69] Andrew Geil, Glen Sagers, Aslihan D. Spaulding, and James R. Wolf. 2018. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *17th Australian Cyber Warfare Conference (CWAR)* 21, 3 (2018), 317–334. https://doi.org/10.22434/IFAMR2017.0045

[70] Eliza M. Grames, Andrew N. Stillman, Morgan W. Tingley, and Chris S. Elphick. 2019. An automated approach to identifying search terms for systematic reviews using keyword co–occurrence networks. *Methods in Ecology and Evolution* 10, 10 (2019), 1645–1654. https://doi.org/10.1111/2041-210X.13268

[71] Md. Habibur Rahman, Md. Al-Amin, and Nusrat Sharmin Lipy. 2020. An Investigation on The Intention to Adopt Mobile Banking on Security Perspective in Bangladesh. *Risk and Financial Management* 2, 2 (2020), 47–58. https://doi.org/10.30560/rfm.v2n2p47

[72] Ziad M. Hakim, Natalie C. Ebner, Daniela S. Oliveira, Sarah J. Getz, Bonnie E. Levin, Tian Lin, Kaitlin Lloyd, Vicky T. Lai, Matthew D. Grilli, and Robert C. Wilson. 2021. The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods* 53, 3 (2021), 1342–1352. https://doi.org/10.3758/s13428-020-01495-0

[73] Tzipora Halevi, Trishank Karthik Kuppusamy, Meghan Caiazzo, and Nasir Memon. 2015. Investigating users' readiness to trade-off biometric fingerprint data. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*. IEEE, Hong Kong, China, 1–8. https://doi.org/10.1109/ISBA.2015.7126366

[74] Nathan B. Hansen, Michael J. Lambert, and Evan M. Forman. 2002. The psychotherapy dose-response effect and its implications for treatment delivery services. *Clinical Psychology: Science and Practice* 9, 3 (2002), 329–343. https://doi.org/10.1093/clipsy.9.3.329

[75] Wu He, Ivan Ash, Mohd Anwar, Ling Li, Xiaohong Yuan, Li Xu, and Xin Tian. 2020. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital* 21, 2 (2020), 203–213. https://doi.org/10.1108/jic-05-2019-0112

[76] Wu He, Xiaohong Yuan, and Xin Tian. 2014. The Self-Efficacy Variable in Behavioral Information Security Research. In *ES '14*. IEEE Computer Society, Shanghai, China, 28–32. https://doi.org/10.1109/ES.2014.52

[77] John W. Henry and Robert W. Stone. 1997. The development and validation of computer self-efficacy and outcome expectancy scales in a nonvolitional context. *Behavior Research Methods, Instruments, & Computers* 29, 4 (1997), 519–527. https://doi.org/10.3758/BF03210603

[78] Tejaswini Herath and H. Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125. https://doi.org/10.1057/ejis.2009.6

[79] Duncan Hodges and Oliver Buckley. 2017. Its Not All About the Money: Self-efficacy and Motivation in Defensive and Offensive Cyber Security Professionals. In *International Conference on Human Aspects of Information Security, Privacy and Trust*, Theo Tryfonas (Ed.). Springer International Publishing, Vancouver, BC, Canada, 494–506.

[80] Gordon Hodson. 2021. Construct jangle or construct mangle? Thinking straight about (nonredundant) psychological constructs. *Journal of Theoretical Social Psychology* 5, 4 (2021), 576–590. https://doi.org/10.1002/jts5.120

[81] Tammy C. Hoffmann, Paul P. Glasziou, Isabelle Boutron, Ruairidh Milne, Rafael Perera, David Moher, Douglas G. Altman, Virginia Barbour, Helen Macdonald, Marie Johnston, Sarah E. Lamb, Mary Dixon-Woods, Peter McCulloch, Jeremy C. Wyatt, An-Wen Chan, and Susan Michie. 2014. Better reporting of interventions: template for intervention description and replication (TIDieR) checklist and guide. *BMJ* 348 (2014), g1687. https://doi.org/10.1136/bmj.g1687 arXiv:https://www.bmj.com/content/348/bmj.g1687.full.pdf

[82] Yvonne Hong and Lesley Gardner. 2014. Facebook groups: Perception and usage among undergraduates in the context of learning. In *ICIS 2014 Proceedings*. AIS, Auckland, New Zeeland, 1–18. https://aisel.aisnet.org/icis2014/proceedings/ISCurriculum/21/

[83] Ashley R. Hopkins. 2019. *Privacy Within Photo-Sharing and Gaming Applications: Motivation and Opportunity and the Decision to Download*. Unpublished doctoral dissertation. Ohio University, Athens, OH, USA.

[84] Kasper Hornbæk, Søren S. Sander, Javier Andrés Bargas-Avila, and Jakob Grue Simonsen. 2014. Is Once Enough? On the Extent and Content of Replications in Human-Computer Interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 3523–3532. https://doi.org/10.1145/2556288.2557004

[85] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[86] Princely Ifinedo, Nigussie Mengesha, and Rahel Bekele. 2022. Effects of Personal Factors and Organizational Reinforcing Tools in Decreasing Employee Engagement in Unhygienic Cyber Practices. *Journal of Global Information Management* 30, 1 (2022), 1–27. https://doi.org/10.4018/JGIM.299324

[87] Harald Janson and Ulf Olsson. 2001. A Measure of Agreement for Interval or Nominal Multivariate Observations. *Educational and Psychological Measurement* 61, 2 (2001), 277–289. https://doi.org/10.1177/00131640121971239

[88] Jongkil Jeong, Joanne Mihelcic, Gillian Oliver, and Carsten Rudolph. 2019. Towards an Improved Understanding of Human Factors in Cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, Los Angeles, California, USA, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

[89] Oliver P. John, Laura P. Naumann, and Christopher J. Soto. 2008. Paradigm shift to the integrative big five trait taxonomy: History, Measurement, and Conceptual Issues. In *Handbook of Personality: Theory and Research*, Oliver P. John, Richard W. Robins, and Lawrence A. Pervin (Eds.). Guilford Press, New York, NY, USA, 14–158.

[90] Keith S. Jones, Natalie R. Lodinger, Benjamin P. Widlus, Akbar Siami Namin, and Rattikorn Hewett. 2021. Do Warning Message Design Recommendations Address Why Non-Experts Do Not Protect Themselves from Cybersecurity Threats? A Review. *International Journal of Human–Computer Interaction* 37, 18 (2021), 1709–1719. https://doi.org/10.1080/10447318.2021.1908691

[91] Hyunjin Kang and Jeeyun Oh. 2023. Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society* 25, 5 (2023), 1153–1175. https://doi.org/10.1177/14614448211026611

[92] Fredrik Karlsson, Martin Karlsson, and Joachim Åström. 2017. Measuring employees' compliance – the importance of value pluralism. *Information & Computer Security* 25, 3 (2017), 279–299. https://doi.org/10.1108/ICS-11-2016-0084

[93] Naurin Farooq Khan, Amber Yaqoob, Muhammad Saud Khan, and Naveed Ikram. 2022. The cybersecurity behavioral research: A tertiary study. *Computers & Security* 120 (2022), 102826. https://doi.org/10.1016/j.cose.2022.102826

[94] Kyongseok Kim and Jooyoung Kim. 2011. Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust. *Journal of Interactive Marketing* 25, 3 (2011), 145–158. https://doi.org/10.1016/j.intmar.2010.09.003

[95] Victoria Kisekka and Sanjay Goel. 2023. An Investigation of the Factors that Influence Job Performance During Extreme Events: The Role of Information Security Policies. *Information Systems Frontiers* 25, 4 (2023), 1439–1458. https://doi.org/10.1007/s10796-022-10281-6

[96] Marion Koelle, Swamy Ananthanarayan, and Susanne Boll. 2020. Social Acceptability in HCI: A Survey of Methods, Measures, and Design Strategies. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–19. https://doi.org/10.1145/3313831.3376162

[97] Kuang Ming Kuo, Yu Chang Chen, Paul C. Talley, and Chi Hsien Huang. 2018. Continuance compliance of privacy policy of electronic medical records: the roles of both motivation and habit. *BMC medical informatics and decision making* 18, 1 (2018), 135. https://doi.org/10.1186/s12911-018-0722-7

[98] Laura Lacalle, Melissa Liher Martínez-Shaw, Yolanda Marín, and Yolanda Sánchez-Sandoval. 2023. Intelligence Quotient (IQ) in school-aged preterm infants: A systematic review. *Frontiers in psychology* 14 (2023), 1216825. https://doi.org/10.3389/fpsyg.2023.1216825

[99] Robert LaRose and Nora J. Rifon. 2007. Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs* 41, 1 (2007), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

[100] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work (USAB) (Lecture Notes in Computer Science, Vol. 5298)*, Andreas Holzinger (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. https://doi.org/10.1007/978-3-540-89350-9{_}6

[101] Ryo-Whoa Lee, Seung-Hyuk Choi, and Sung-Ho Hu. 2023. Effect of temporal distance and goal type on predictions of future information security: Focus on moderation of self-efficacy and social responsibility. *Acta psychologica* 238 (2023), 103990. https://doi.org/10.1016/j.actpsy.2023.103990

[102] Ling Li, Li Xu, and Wu He. 2022. The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports* 5 (2022), 100165. https://doi.org/10.1016/j.chbr.2021.100165

[103] Scott O. Lilienfeld and Adele N. Strother. 2020. Psychological measurement and the replication crisis: Four sacred cows. *Canadian Psychology/Psychologie canadienne* 61, 4 (2020), 281–288. https://doi.org/10.1037/cap0000236

[104] Jing Liu, Marko M. Skoric, and Chen Li. 2023. Disentangling the relation among trust, efficacy and privacy management: a moderated mediation analysis of public support for government surveillance during the COVID-19 pandemic. *Behaviour & Information Technology* Ahead of Print (2023), 1–20. https://doi.org/10.1080/0144929X.2023.2178830

[105] Kate Miriam Loewenthal and Christopher Alan Lewis. 2020. *An introduction to psychological tests and scales*. Routledge, London, UK. https://doi.org/10.4324/9781315561387

[106] Rubén López-Nicolás, José Antonio López-López, María Rubio-Aparicio, and Julio Sánchez-Meca. 2022. A meta-review of transparency and reproducibility-related reporting practices in published meta-analyses on clinical psychological interventions (2000-2020). *Behavior Research Methods* 54, 1 (2022), 334–349. https://doi.org/10.3758/s13428-021-01644-z

[107] Ricardo G. Lugo, Benjamin J. Knox, Øyvind Josøk, and Stefan Sütterlin. 2020. Variable Self-Efficacy as a Measurement for Behaviors in Cyber Security Operations. In *Augmented Cognition. Human Cognition and Behavior*, Dylan D. Schmorrow (Ed.). Springer International Publishing AG, Cham, 395–404.

[108] Xin Luo, Han Li, Qing Hu, and Heng Xu. 2020. Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective. *Journal of the Association for Information Systems* 21, 6 (2020), 1552–1593. https://doi.org/10.17705/1jais.000646

[109] Rachid A. Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. 2020. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* 3 (2020), 10. https://doi.org/10.1186/s42400-020-00050-w

[110] Stanislav Mamonov and Marios Koufaris. 2016. The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security* 12, 2 (2016), 1–12. https://doi.org/10.1080/15536548.2016.1163026

[111] George Marakas, Richard Johnson, and Paul Clay. 2007. The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time. *Journal of the Association for Information Systems* 8, 1 (2007), 16–46. https://doi.org/10.17705/1jais.00112

[112] Monica M. McGill, Sarah B. Lee, Litany Lineberry, John Sands, and Leigh Ann DeLyser. 2021. Piloting the Air Force JROTC Cyber Academy for High School Students. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21)*. Association for Computing Machinery, New York, NY, USA, 597–603. https://doi.org/10.1145/3408877.3432471

[113] Tanya McGill and Nik Thompson. 2017. Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology* 36, 11 (2017), 1111–1124. https://doi.org/10.1080/0144929X.2017.1352028

[114] Yannic Meier and Nicole Krämer. 2023. Differences in Access to Privacy Information Can Partly Explain Digital Inequalities in Privacy Literacy and Self-Efficacy: Preprint. https://doi.org/10.31234/osf.io/se57p

[115] Helfried Moosbrugger. 2012. *Testtheorie und Fragebogenkonstruktion* (2., aktualisierte und überarbeitete auflage ed.). Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20072-4

[116] Florence Mwagwabi, Tanya McGill, and Mike Dixon. 2018. Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems* 42 (2018), 147–182. https://doi.org/10.17705/1CAIS.04207

[117] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie C. Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46, 4 (2009), 815–825.

[118] Matthew Oakley, Sam Mohun Himmelweit, Paul Leinster, and Mónica Casado. 2020. Protection Motivation Theory: A Proposed Theoretical Extension and Moving beyond Rationality—The Case of Flooding. *Water* 12, 7 (2020), 1848. https://doi.org/10.3390/w12071848

[119] Open Science Collaboration. 2015. Estimating the reproducibility of psychological science. *Science* 349, 6251 (2015), aac4716. https://doi.org/10.1126/science.aac4716

[120] Dorottya Papp, Kristóf Tamás, and Levente Buttyán. 2019. IoT Hacking – A Primer. *Infocommunications Journal* 11, 2 (2019), 2–13. https://doi.org/10.36244/ICJ.2019.2.1

[121] Robert A. Peterson and Yeolib Kim. 2013. On the relationship between coefficient alpha and composite reliability. *The Journal of Applied Psychology* 98, 1 (2013), 194–198. https://doi.org/10.1037/a0030767

[122] Jonathan A. Plucker and Matthew C. Makel. 2021. Replication is important for educational psychology: Recent developments and key issues. *Educational Psychologist* 56, 2 (2021), 90–100. https://doi.org/10.1080/00461520.2021.1895796

[123] Livia Puljak. 2019. Methodological studies evaluating evidence are not systematic reviews: Letter to the Editor. *Journal of Clinical Epidemiology* 110, 6 (2019), 98–99. https://doi.org/10.1016/j.jclinepi.2019.02.002

[124] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction* 30 (2021), 100343. https://doi.org/10.1016/j.ijcci.2021.100343

[125] Sarah M. Rajtmajer, Timothy M. Errington, and Frank G. Hillary. 2022. How failure to falsify in high-volume science contributes to the replication crisis. *eLife* 11 (2022), 1–13. https://doi.org/10.7554/eLife.78830

[126] Kevin L. Rand. 2018. Hope, self-efficacy, and optimism: Conceptual and empirical differences. In *The Oxford handbook of hope*, Matthew W. Gallagher and Shane J. Lopez (Eds.). Oxford University Press, New York, NY, USA, 45–58.

[127] John Raven, Jean C. Raven, and John H. Court. 2000. *Manual for Raven's Progressive Matrices and Vocabulary Scales* (sections 1 to 7with three research appendices ed.). Harcourt Assessment, San Antonio,TX, USA.

[128] Dinesh Reddy and Glenn Dietrich. 2019. Unlocking the Mixed Results of the Effect of Self-Efficacy in Information Security on Compliance. In *AMCIS 2019 Proceedings*. AIS, Cancun, Mexico, 31. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/31

[129] Hyeun-Suk Rhee, Cheongtag Kim, and Young U. Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security* 28, 8 (2009), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

[130] Wendy M. Rodgers, David Markland, Anne-Marie Selzler, Terra C. Murray, and Philip M. Wilson. 2014. Distinguishing perceived competence and self-efficacy: an example from exercise. *Research Quarterly for Exercise and Sport* 85, 4 (2014), 527–539. https://doi.org/10.1080/02701367.2014.961050

[131] Katja Rogers and Katie Seaborn. 2023. The systematic review-lution: A manifesto to promote rigour and inclusivity in research synthesis. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson, and Anicia Peters (Eds.). ACM, New York, NY, USA, 1–11. https://doi.org/10.1145/3544549.3582733

[132] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology* 91, 1 (1975), 93–114. https://doi.org/10.1080/00223980.1975.9915803

[133] Rohani Rohan, Suree Funilkul, Debajyoti Pal, and Wichian Chutimaskul. 2021. Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. In *2021 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, Shillong, Meghalaya, India, 133–140. https://doi.org/10.1109/ComPE53109.2021.9752358

[134] Irwin M. Rosenstock. 1966. Why People Use Health Services. *The Milbank Memorial Fund Quarterly* 44, 3 (1966), 94–124. https://doi.org/10.2307/3348967

[135] Irwin M. Rosenstock, Victor J. Strecher, and Marshall H. Becker. 1988. Social learning theory and the Health Belief Model. *Health Education Quarterly* 15, 2 (1988), 175–183. https://doi.org/10.1177/109019818801500203

[136] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78. https://doi.org/10.1016/j.cose.2015.05.012

[137] Kavous Salehzadeh Niksirat, Lahari Goswami, Pooja S. B. Rao, James Tyler, Alessandro Silacci, Sadiq Aliyu, Annika Aebli, Chat Wacharamanotham, and Mauro Cherubini. 2023. Changes in Research Ethics, Openness, and Transparency in Empirical Studies between CHI 2017 and CHI 2022. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson, Anicia Peters, Stefanie Mueller, Julie R. Williamson, and Max L. Wilson (Eds.). ACM, New York, NY, USA, 1–23. https://doi.org/10.1145/3544548.3580848

[138] Antti Salovaara and Jani Merikivi. 2015. IS Research Progress Would Benefit from Increased Falsification of Existing Theories. In *ECIS 2015 completed research papers*. AIS, Münster, Germany, 157.

[139] Antti Salovaara, Bikesh Raj Upreti, Jussi Ilmari Nykänen, and Jani Merikivi. 2020. Building on shaky foundations? Lack of falsification and knowledge contestation in IS theories, methods, and practices. *European Journal of Information Systems* 29, 1 (2020), 65–83. https://doi.org/10.1080/0960085X.2019.1685737

[140] Puspita Kencana Sari, Putu Wuri Handayani, Achmad Nizar Hidayanto, Setiadi Yazid, and Rizal Fathoni Aji. 2022. Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. *Healthcare (Basel, Switzerland)* 10, 12 (2022), 1–21. https://doi.org/10.3390/healthcare10122531

[141] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting IT-Security: How Organisations Can Encourage and Sustain Secure Behaviours. In *27th European Symposium on Research in Computer Security*. Springer, Copenhagen, Denmark, 248––265.

[142] Lothar Schmidt-Atzert, Manfred Amelang, Thomas Fydrich, and Helfried Moosbrugger. 2018. *Psychologische Diagnostik* (5. ed.). Springer, Berlin and Heidelberg, Germany. https://doi.org/10.1007/978-3-642-17001-0
[143] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2017. Construction of a Benchmark for the User Experience Questionnaire (UEQ). *International Journal of Interactive Multimedia and Artificial Intelligence* 4, 4 (2017), 40. https://doi.org/10.9781/ijimai.2017.445
[144] Richard H. Scotts. 2020. *Cyber security in mental health: An assessment of current practice and behavioral intent: Dissertation.* ProQuest LLC, Ann Arbor, MI, USA.
[145] Willie C. Session. 2022. *Cybersecurity Leadership: Technology Threat Avoidance Factors Affecting Cybersecurity Professionals' Willingness to Share Information.* ProQuest Dissertations Publishing, Ann Arbor, MI, USA. https://www.proquest.com/dissertations-theses/cybersecurity-leadership-technology-threat/docview/2731014190/se-2
[146] Filipo Sharevski, Paige Treebridge, and Jessica Westbrook. 2019. Experiential User-Centered Security in a Classroom: Secure Design for IoT. *IEEE Communications Magazine* 57, 11 (2019), 48–53. https://doi.org/10.1109/MCOM.001.1900223
[147] Sarah Sharifi. 2023. A Novel Approach to the Behavioral Aspects of Cybersecurity. https://doi.org/10.48550/arXiv.2303.13621
[148] Mario Silic. 2017. Explaining Organizational Employee Computer Abuse Through an Extended Health Belief Model. *SSRN Electronic Journal* 24 (2017), 1–37. https://doi.org/10.2139/ssrn.3070823
[149] Mikko Siponen, Seppo Pahnila, and Adam Mahmood. 2007. Employees' Adherence to Information Security Policies: An Empirical Study. In *New Approaches for Security, Privacy and Trust in Complex Environments (IFIP International Federation for Information Processing, Vol. 232)*, Hein Venter, Jan Eloff, Mariki Eloff, Les Labuschagne, and Rossouw Solms (Eds.). International Federation for Information Processing, Boston, MA, USA, 133–144. https://doi.org/10.1007/978-0-387-72367-9{_}12
[150] Ellen A. Skinner. 1996. A guide to constructs of control. *Journal of Personality and Social Psychology* 71, 3 (1996), 549–570. https://doi.org/10.1037/0022-3514.71.3.549
[151] Karen H. Smith, Francis A. Méndez Mediavilla, and Garry L. White. 2018. The Impact of Online Training on Facebook Privacy. *Journal of Computer Information Systems* 58, 3 (2018), 244–252. https://doi.org/10.1080/08874417.2016.1233001
[152] Jeffrey Stanton, Paul Mastrangelo, Kathryn Stam, and Jeffrey Jolton. 2004. Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. In *Proceedings of the Tenth Americas Conference on Information Systems, AMCIS 2004*, Association for Information Systems (Ed.). AIS Electronic Library, New York, NY, USA, 1388–1394.
[153] Evropi Stefanidi, Marit Bentvelzen, Paweł W. Woźniak, Thomas Kosch, Mikołaj P. Woźniak, Thomas Mildner, Stefan Schneegass, Heiko Müller, and Jasmin Niess. 2023. Literature Reviews in HCI: A Review of Reviews. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson, Anicia Peters, Stefanie Mueller, Julie R. Williamson, and Max L. Wilson (Eds.). ACM, New York, NY, USA, 1–24. https://doi.org/10.1145/3544548.3581332
[154] Noor Suhani Sulaiman, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. *Social Sciences* 11, 9 (2022), 386. https://doi.org/10.3390/socsci11090386
[155] Shane N. Sweet, Michelle S. Fortier, Shaelyn M. Strachan, and Chris M. Blanchard. 2012. Testing and integrating self-determination theory and self-efficacy theory in a physical activity context. *Canadian Psychology/Psychologie canadienne* 53, 4 (2012), 319–327. https://doi.org/10.1037/a0030280
[156] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security* 70 (2017), 376–391. https://doi.org/10.1016/j.cose.2017.07.003
[157] Iris van Ooijen, Claire M. Segijn, and Suzanna J. Opree. 2022. Privacy Cynicism and its Role in Privacy Decision-Making: OnlineFirst. *Communication Research* 0: Ahead of Print (2022), 1–32. https://doi.org/10.1177/00936502211060984
[158] Silas Formunyuy Verkijika. 2019. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior* 101 (2019), 286–296. https://doi.org/10.1016/j.chb.2019.07.034
[159] Chat Wacharamanotham, Lukas Eisenring, Steve Haroz, and Florian Echtler. 2020. Transparency of CHI Research Artifacts: Results of a Self-Reported Survey. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Regina Bernhaupt, Florian 'Floyd' Mueller, David Verweij, Josh Andres, Joanna McGrenere, Andy Cockburn, Ignacio Avellino, Alix Goguey, Pernille Bjørn, Shengdong Zhao, Briane Paul Samson, and Rafal Kocielnik (Eds.). ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376448
[160] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for facebook. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, Matt Jones, Philippe Palanque, Albrecht Schmidt, and Tovi Grossman (Eds.). ACM Press, New York, New York, USA, 2367–2376. https://doi.org/10.1145/2556288.2557413
[161] Aaron C. Weidman, Conor M. Steckler, and Jessica L. Tracy. 2017. The jingle and jangle of emotion assessment: Imprecise measurement, casual scale usage, and conceptual fuzziness in emotion research. *Emotion* 17, 2 (2017), 267–295. https://doi.org/10.1037/emo0000226
[162] Yana Weinstein. 2018. Mind-wandering, how do I measure thee with probes? Let me count the ways. *Behavior Research Methods* 50, 2 (2018), 642–661. https://doi.org/10.3758/s13428-017-0891-9
[163] David A. Wilkerson, Samantha N. Wolfe-Taylor, and M. Killian Kinney. 2021. Adopting e-Social Work Practice: Pedagogical Strategies for Student Decision Making to Address Technology Uncertainty. *Journal of Social Work Education* 57, 2 (2021), 383–397. https://doi.org/10.1080/10437797.2019.1661920
[164] Anja Wittkowski, Charlotte Garrett, Rachel Calam, and Daniel Weisberg. 2017. Self-report measures of parental self-efficacy: A systematic review of the current literature. *Journal of Child and Family Studies* 26, 11 (2017), 2960–2978. https://doi.org/10.1007/s10826-017-0830-5
[165] Donghee Yvette Wohn and Chandan Sarkar. 2012. Expertise Matters: Privacy Perceptions and Practices in Response to Behavioral Targeting. *SSRN Electronic Journal* 19 (2012), 1–30. https://doi.org/10.2139/ssrn.2046739
[166] Peera Wongupparaj, Veena Kumari, and Robin G. Morris. 2015. A Cross-Temporal Meta-Analysis of Raven's Progressive Matrices: Age groups and developing versus developed countries. *Intelligence* 49 (2015), 1–9. https://doi.org/10.1016/j.intell.2014.11.008
[167] Michael Workman, William H. Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24, 6 (2008), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005
[168] Seounmi Youn. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs* 43, 3 (2009), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x
[169] Brahim Zarouali, Karolien Poels, Koen Ponnet, and Michel Walrave. 2018. "Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. *Cyberpsychology Journal of Psychosocial Research on Cyberspace* 12, 1 (2018), 5. https://doi.org/10.5817/cp2018-1-5
[170] Leah Zhang-Kennedy and Sonia Chiasson. 2022. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *Comput. Surveys* 54, 1 (2022), 1–39. https://doi.org/10.1145/3427920
[171] Guangyu Zhou, Mengke Gou, Yiqun Gan, and Ralf Schwarzer. 2020. Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage. *Frontiers in Psychology* 11 (2020), 1066. https://doi.org/10.3389/fpsyg.2020.01066

A PEER-REVIEWED AND NON-PEER-REVIEWED PUBLICATIONS

Table A1 in this Appendix shows results of key variables of interest when separate analyses were run for peer-reviewed and non-peer-reviewed publications. Please note that, e.g., non-peer-reviewed publications report a higher number of scales in relation to the number of publications compared to peer-reviewed publications.

B MEASURE-SPECIFIC METHODOLOGICAL RIGOR

Table B1 and Table B2 in this Appendix show whether or not information about certain criteria that concern the rigor of the scale development process was reported in sufficient detail; for first use and recurring measures respectively. The Tables are arranged by scale number for easier comparison of related measures.

C NEWLY CREATED AND ADAPTED MEASURES

Table C1 in this Appendix presents the outcomes for key variables of interest from separate analyses conducted for both newly created and adapted measures. We categorized measures as newly created if they did not report original authors for their item compositions.

D CYBERSECURITY SE RESEARCH FRAMEWORKS

The three Tables in this Appendix list all the identified and collapsed variables that are hypothesized to either influence cybersecurity SE (see Table D1), be influenced by cybersecurity SE (see Table D2), or both (see Table D3). Tables are sorted by frequency and then in alphabetical order.

APPENDIX REFERENCES

[172] Nahil Abdallah, Odeh Abdalla, Hamzah Alkhazaleh, and Amer Ibrahim. 2020. Information security awareness behavior among higher education students: Case study. *Journal of Theoretical and Applied Information Technology* 98, 18 (2020), 3825–3836. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092632608&partnerID=40&md5=3824881bcf0480c8de6cc33dce0261e2

[173] Sherly Abraham. 2012. *Exploring the effectiveness of information security training and persuasive messages*. Vol. 74. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2013-99230-514&site=ehost-live

[174] Sherly Abraham and InduShobha Chengalur-Smith. 2019. Evaluating the effectiveness of learner controlled information security training. *Computers & Security* 87 (2019), 101586. https://doi.org/10.1016/j.cose.2019.101586

[175] John Agyekum Addae, Grace Simpson, and George Oppong Appiagyei Ampong. 2019. Factors Influencing Information Security Policy Compliance Behavior. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*. IEEE, Accra, Ghana, 43–47. https://doi.org/10.1109/ICSIoT47925.2019.00015

[176] Kishalay Adhikari and Rajeev Kumar Panda. 2018. Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing* 31, 2 (2018), 1–15. https://doi.org/10.1080/08911762.2017.1412552

[177] Zauwiyah Ahmad, Thian Song Ong, Tze Hui Liew, and Mariati Norhashim. 2019. Security monitoring and information security assurance behaviour among employees. *Information and Computer Security* 27, 2 (2019), 165–188. https://doi.org/10.1108/ics-10-2017-0073

[178] Mofleh Al-diabat. 2018. Investigating the Determinants of College Students Information Security Behavior Using a Validated Multiple Regression Models. *International Journal of Computer Science and Information Technology* 10, 6 (2018), 81–96. https://doi.org/10.2139/ssrn.3336446

[179] Sultan T. Alanazi, Mohammed Anbar, Shouki A. Ebad, Shankar Karuppayah, and Hadeer A. Al-Ani. 2020. Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry* 12, 9 (2020), 1544. https://doi.org/10.3390/sym12091544

[180] Samar Muslah Albladi and George R. S. Weir. 2017. Competence measure in social networks. In *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, Madrid, Spain, 1–6. https://doi.org/10.1109/CCST.2017.8167845

[181] Abdullah Almuqrin. 2018. *Examining the influence of technology acceptance, self-efficacy, and locus of control on information security behavior of social media users*. Vol. 80. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2019-23494-039&site=ehost-live

[182] Amani Alqarni. 2017. *Exploring factors that affect adoption of computer security practices among college students*. Vol. 763. Master's Theses and Doctoral Dissertations, Ypsilanti, MI, USA. http://commons.emich.edu/theses/763

[183] Yazan Alshboul and Kevin Streff. 2017. Beyond Cybersecurity Awareness: Antecedents and Satisfaction. In *Proceedings of the 2017 International Conference on Software and E-Business (ICSEB 2017)*. Association for Computing Machinery, New York, NY, USA, 85–91. https://doi.org/10.1145/3178212.3178218

[184] Ahmad Alturki, Nora Alshwihi, and Abdulla Algarni. 2020. Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks. *IEEE Access* 8 (2020), 97383–97391. https://doi.org/10.1109/ACCESS.2020.2995619

[185] Laura Amo. 2016. Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy. *IEEE Security & Privacy* 14, 1 (2016), 72–75. https://doi.org/10.1109/MSP.2016.12

[186] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69 (2017), 437–443. https://doi.org/10.1016/j.chb.2016.12.040

[187] Nalin Asanka Gamagedara Arachchilage. 2016. *Serious Games for Cyber Security Education*. LAP LAMBERT, Academic Publishing, London, UK. https://app.dimensions.ai/details/publication/pub.1118620894

[188] Salvatore Aurigemma. 2013. *From the weakest link to the best defense: Exploring the factors that affect employee intention to comply with information security policies*. Vol. 74. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2014-99100-433&site=ehost-live

[189] Salvatore Aurigemma and Thomas Mattson. 2015. The Role of Social Status and Controllability on Employee Intent to Follow Organizational Information Security Requirements. In *2015 48th Hawaii International Conference on System Sciences*. IEEE, Kauai, HI, USA, 3527–3536. https://doi.org/10.1109/HICSS.2015.424

[190] Emmanuel W. Ayaburi, James Wairimu, and Francis Kofi Andoh-Baidoo. 2019. Antecedents and Outcome of Deficient Self-Regulation in Unknown Wireless Networks Use Context: An Exploratory Study. *Information Systems Frontiers* 21, 6 (2019), 1213–1229. https://doi.org/10.1007/s10796-019-09942-w

[191] France Belanger and Robert E. Crossler. 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems* 28, 1 (2019), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

[192] Ardion Beldad. 2016. Sealing One's Online Wall Off From Outsiders: Determinants of the Use of Facebook's Privacy Settings among Young Dutch Users. *International Journal of Technology and Human Interaction* 12, 1 (2016), 21–34. https://doi.org/10.4018/ijthi.2016010102

[193] Richard Scott Bell, Eugene Vasserman, and Eleanor C. Sayre. 2014. A longitudinal study of students in an introductory cybersecurity course. In *121st ASEE Annual Conference & Exposition*. American Society for Engineering Education, Indianapolis, IN, USA, 1–11.

[194] Richard Scott Bell, Eugene Vasserman, and Eleanor C. Sayre. 2015. Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses. In *122nd ASEE Annual Conference and Exposition: Making Value for Society*. American Society for Engineering Education, Indianapolis, IN, USA, 1–13.

[195] Jean-Francois Berthevas. 2018. Students' computers safety behaviors, under effects of cognition and socialization: When gender and job experience influence information security behaviors. In *2018 IEEE International Conference on Technology Management, Operations and Decisions (Ictmod)*. IEEE, Marrakech, Morocco, 244–251.

[196] Goli Marius Beugré. 2019. *Perceived behaviors and security compliance intention of employees processing big data: A correlational study*. Vol. 81. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-04047-121&site=ehost-live

[197] John M. Blythe and Lynne Coventry. 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior* 87 (2018), 87–97. https://doi.org/10.1016/j.chb.2018.05.023

[198] Hanieh Yaghoobi Bojmaeh. 2015. Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior. *International Journal of Science and Engineering Applications* 4, 6 (2015), 361–365. https://doi.org/10.7753/ijsea0406.1006

[199] Cheryl Booth and Shuyuan Mary Ho. 2019. The Privacy Paradox in HCI: Calculus Behavior in Disclosing PII Online. In *6th International Conference, HCI in Business, Government and Organizations 2019*. Springer-Verlag, Orlando, FL, USA, 163–177.

[200] Cheryl Lynn Booth. 2019. *Tipping the balance in privacy calculus: The roles of perceived trustworthiness, uncertainty, and cyber self-efficacy in an online user's intention to disclose PII*. Dissertation. Florida State University, Tallahassee, FL, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-28117-060&site=ehost-live

[201] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Mis Quarterly* 34, 3 (2010), 523–548.

[202] Kristen A. Carruth and Harvey J. Ginsburg. 2017. Social networking and privacy attitudes among college students. *Psychology Society & Education* 6, 2 (2017), 82. https://doi.org/10.25115/psye.v6i2.510

[203] Nadire Cavus and Erinc Ercag. 2016. The scale for the self–efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology* 47, 1 (2016), 76–90. https://doi.org/10.1111/bjet.12217

[204] Nadire Cavus and Alaa A. Mohammed. 2017. Scale for Efficacy in the Safe Use of the Internet for Students. In *5th Cyprus International Conference Educational Research*. New Trends and Issues Proceedings on Humanities and Social Sciences, Kyrenia, Cyprus, 227–234.

[205] Hao Chen, Ofir Turel, and Yufei Yuan. 2021. E-waste information security protection motivation: the role of optimism bias. *Information Technology and People* 35, 2 (2021), 600–620. https://doi.org/10.1108/itp-09-2019-0458

[206] Hsuan-Ting Chen. 2018. Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist* 62, 10 (2018), 1392–1412. https://doi.org/10.1177/0002764218792691

[207] Hsuan-Ting Chen and Wenhong Chen. 2015. Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology Behavior and Social Networking* 18, 1 (2015), 13–19. https://doi.org/10.1089/cyber.2014.0456

[208] Tianying Chen, Margot Stewart, Zhiyu Bai, Eileen Chen, Laura Dabbish, and Jessica Hammer. 2020. Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference (DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1737–1749. https://doi.org/10.1145/3357236.3395522

[209] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 503–514. https://doi.org/10.1145/2818048.2819996

[210] Hui-Lien Chou and Chien Chou. 2016. An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior* 65 (2016), 334–345. https://doi.org/10.1016/j.chb.2016.08.034

[211] Hui-Lien Chou and Jerry Chih-Yuan Sun. 2017. The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education* 112 (2017), 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

[212] Christine Y. Clark. 2013. *A study on corporate security awareness and compliance behavior intent*. Vol. 74. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2014-99091-417&site=ehost-live

[213] Robert E. Crossler. 2010. Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. In *43rd Hawaii International Conference on System Sciences*. IEEE, Honolulu, HI, USA, 1–10. https://doi.org/10.1109/HICSS.2010.311

[214] Robert E. Crossler and France Bélanger. 2019. Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research* 30, 3 (2019), 995–1006. https://doi.org/10.1287/isre.2019.0846

[215] Suresh Cuganesan, Cara Steele, and Alison Hart. 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour and Information Technology* 37, 1 (2018), 1–16. https://doi.org/10.1080/0144929x.2017.1397193

[216] Duy Dang-Pham and Siddhi Pittayachawan. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security* 48 (2015), 281–297. https://doi.org/10.1016/j.cose.2014.11.002

[217] Robert K. Day. 2018. *Modeling the influence of personal characteristics on information security policy compliance in US-based financial, medical, and information services industries*. Vol. 79. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2018-26094-231&site=ehost-live

[218] Vipan Devgan. 2012. *Satisfactions, self-efficacy, and compliance in mandatory technology settings*. Vol. 74. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2013-99130-329&site=ehost-live

[219] Charlette Donalds and Kweku-Muata Osei-Bryson. 2020. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management* 51 (2020), 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

[220] Kristi C. Dorsey-Lockett. 2014. *Examining the correlation between organizational security climate and demographic variables and the self-efficacy of information security of local government employees: A quantitative study*. Vol. 75. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2015-99020-274&site=ehost-live

[221] Marc Dupuis. 2019. Going Back for that One Last Thing in the House on Fire: How Fear, Attentiveness, Sadness, Joviality, and Other Lower Order Dimensions of Affect Influence Our Security and Privacy Behavior. In *2019 IEEE SmartWorld 2019*. IEEE, Leicester, UK, 1825–1833. https://doi.org/10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00322

[222] Marc J. Dupuis. 2014. *The role of trait affect in the information security behavior of home users*. Vol. 75. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2015-99110-190&site=ehost-live

[223] Esther Dzidzah, Kwame Owusu Kwateng, and Benjamin Kofi Asante. 2020. Security behaviour of mobile financial service users. *Information and Computer Security* 28, 5 (2020), 719–741. https://doi.org/10.1108/ics-02-2020-0021

[224] John D. Elhai, Jason C. Levine, and Brian J. Hall. 2017. Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior. *Internet Research* 27, 3 (2017), 631–649. https://doi.org/10.1108/IntR-03-2016-0070

[225] Chidi Ezuma-Ngwu. 2019. *Exploring individual intent towards blockchain technology in response to threats to personal data and privacy*. Vol. 81. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-31102-001&site=ehost-live

[226] Ali Farooq, Debora Jeske, and Jouni Isoaho. 2019. Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model. In *ICT Systems Security and Privacy Protection*. Springer, Lisbon, Portugal, 238–252. https://doi.org/10.1007/978-3-030-22312-0{_}17

[227] Ali Farooq, Joshua Ndiege, and Jouni Isoaho. 2019. Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. In *2019 IEEE AFRICON*. IEEE, Accra, Ghana, 1–8. https://doi.org/10.1109/AFRICON46755.2019.9133764

[228] Faith B. Fatokun, Suraya Hamid, Azah Norman, and Johnson O. Fatokun. 2019. The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. In *Journal of Physics: Conference Series (JPCS)*. IOP Publishing, Padang, Indonesia, 12098.

[229] Faith B. Fatokun, Suraya Hamid, Azah Norman, Johnson O. Fatokun, and Christopher I. Eke. 2020. Relating Factors of Tertiary Institution Students' Cybersecurity Behavior. In *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*. IEEE, Ayobo, Nigeria, 1–6. https://doi.org/10.1109/ICMCECS47690.2020.246990

[230] Waldo Rocha Flores and Mathias Ekstedt. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security* 59 (2016), 26–44. https://doi.org/10.1016/j.cose.2016.01.004

[231] Ray M. Gagne. 2020. *Motivational factors that cause employees to bypass security: A correlational study*. Vol. 82. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-67313-211&site=ehost-live

[232] Andrew Geil, Glen Sagers, Aslihan D. Spaulding, and James R. Wolf. 2018. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review* 21, 3 (2018), 317–334. https://doi.org/10.22434/ifamr2017.0045

[233] Maryam Ghazi-Asgar, Hamid Reza Peikari, and Asghar Ehteshami. 2018. Health Information Management: Psychological factors influencing information privacy concerns in psychiatric hospitals. *Bali Medical Journal* 7, 1 (2018), 120–126. https://doi.org/10.15562/bmj.v7i1.793

[234] Andrew R. Gillam and W. Tad Foster. 2020. Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior* 108 (2020), 106319. https://doi.org/10.1016/j.chb.2020.106319

[235] Anthony Duke Giwah, Ling Wang, Yair Levy, and Inkyoung Hur. 2020. Empirical assessment of mobile device users' information security behavior towards data breach. *Journal of Intellectual Capital* 21, 2 (2020), 215–233. https://doi.org/10.1108/jic-03-2019-0063

[236] Tzipora Halevi, Trishank K. Kuppusamy, Meghan Caiazzo, and Nasir Memon. 2015. Investigating Users' Readiness to Trade-off Biometric Fingerprint Data. In *2015 IEEE International Conference on Identity, Security and Behavior Analysis (Isba)*. IEEE, Hong Kong, China, 1–8. https://doi.org/10.1109/ISBA.2015.7126366

[237] Tzipora Halevi, Nasir Memon, James Lewis, Ponnurangam Kumaraguru, Sumit Arora, Nikita Dagar, Fadi Aloul, and Jay Chen. 2016. Cultural and Psychological Factors in Cyber-Security. In *Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services (iiWAS '16)*. Association for Computing Machinery, New York, NY, USA, 318–324. https://doi.org/10.1145/3011141.3011165

[238] Chang-Dae Ham. 2017. Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising* 36, 4 (2017), 632–658. https://doi.org/10.1080/02650487.2016.1239878

[239] Bartlomiej Hanus and Yu Wu. 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management* 33, 1 (2016), 2–16. https://doi.org/10.1080/10580530.2015.1117842

[240] Wu He, Ivan Ash, Mohd Anwar, Ling Li, Xiaohong Yuan, Li Xu, and Xin Tian. 2020. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital* 21, 2 (2020), 203–213. https://doi.org/10.1108/jic-05-2019-0112

[241] Barbara Hewitt, Diane Dolezel, and Alexander McLeod. 2017. Mobile Device Security: Perspectives of Future Healthcare Workers. *Perspectives in Health Information Management is* 14, Winter (2017), 1c. https://app.dimensions.ai/details/publication/pub.1085767166

[242] Cho Hichang. 2010. Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies. *Journal of Information Privacy and Security* 6, 1 (2010), 3–27. https://doi.org/10.1080/15536548.2010.10855879

[243] Val Hooper and Chris Blunt. 2020. Factors influencing the information security behaviour of IT employees. *Behaviour and Information Technology* 39, 8 (2020), 1–13. https://doi.org/10.1080/0144929x.2019.1623322

[244] Kong J. Hui, Syarulnaziah Anawar, Nur F. Othman, Zakiah Ayop, and Erman Hamid. 2020. User privacy protection behavior and information sharing in mobile health application. *International Journal of Advanced Trends in Computer Science and Engineering* 9, 4 (2020), 5250–5258. https://doi.org/10.30534/ijatcse/2020/155942020

[245] Norshima Humaidi and Vimala Balakrishnan. 2018. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal* 47, 1 (2018), 17–27. https://doi.org/10.1177/1833358317700255

[246] Norshima Humaidi, Vimala Balakrishnan, and Melissa Shahrom. 2014. Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model. In *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*. IEEE, Hawthorne, VIC, Australia, 30–35.

https://doi.org/10.1109/IC3e.2014.7081237
[247] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95. https://doi.org/10.1016/j.cose.2011.10.007
[248] Khairun Ashikin Ismail, Manmeet Mahinderjit Singh, Norlia Mustaffa, Pantea Keikhosrokiani, and Zakiah Zulkefli. 2017. Security Strategies for Hindering Watering Hole Cyber Crime Attack. In *4th Information Systems International Conference*. Elsevier, Bali, Indonesia, 656–663. https://doi.org/10.1016/j.procs.2017.12.202
[249] Jurjen Jansen and Paul van Schaik. 2018. Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior* 87 (2018), 371–383. https://doi.org/10.1016/j.chb.2018.05.010
[250] Allen C. Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: An empirical study. *Mis Quarterly* 34, 3 (2010), 549–566.
[251] Allen C. Johnston, Barbara Wech, Eric Jack, and Micah Beavers. 2010. Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. In *Proceedings of the Sixteenth Americas Conference on Information Systems*. AISeL, Lima, Peru, 2217–2230. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84870327508&partnerID=40&md5=b4729455201c6b2a685d3ace72756df6
[252] Eunjin Jung, Evelyn Y. Ho, Hyewon Chung, and Mark Sinclair. 2015. Perceived Risk and Self-Efficacy Regarding Internet Security in a Marginalized Community. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 1085–1090. https://doi.org/10.1145/2702613.2732912
[253] Fredrik Karlsson, Martin Karlsson, and Joachim Åström. 2017. Measuring employees' compliance – the importance of value pluralism. *Information and Computer Security* 25, 3 (2017), 279–299. https://doi.org/10.1108/ics-11-2016-0084
[254] Kyongseok Kim and Jooyoung Kim. 2011. Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust. *Journal of Interactive Marketing* 25, 3 (2011), 145–158. https://doi.org/10.1016/j.intmar.2010.09.003
[255] Min Sung Kim and Seongcheol Kim. 2018. Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behavior* 88 (2018), 143–152. https://doi.org/10.1016/j.chb.2018.06.031
[256] Sang Hoon Kim, Kyung Hoon Yang, and Sunyoung Park. 2014. An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal* 2014 (2014), 463870. https://doi.org/10.1155/2014/463870
[257] Alfred Kobsa, Hichang Cho, and Bart P. Knijnenburg. 2016. The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology* 67, 11 (2016), 2587–2606. https://doi.org/10.1002/asi.23629
[258] Daniel Koloseni, Chong Yee Lee, and Gan Ming Lee. 2018. Security police compliance in public institutions: An integrative approach. *Journal of Applied Structural Equation Modeling* 2, 1 (2018), 13–28. https://doi.org/10.47263/jasem.2(1)03
[259] Daniel Ntabagi Koloseni, Chong Yee Lee, and Ming-Lee Gan. 2019. Understanding Information Security Behaviours of Tanzanian Government Employees. *International Journal of Technology and Human Interaction* 15, 1 (2019), 15–32. https://doi.org/10.4018/ijthi.2019010102
[260] Alex Koohang, Jonathan Anderson, Jeretta Horn Nord, and Joanna Paliszkiewicz. 2019. Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems* 120, 1 (2019), 231–247. https://doi.org/10.1108/imds-07-2019-0412
[261] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski (Eds.). 2020. *Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities: Proceedings of the ACM on Human-Computer Interaction (PACMHCI)*. CSCW3, Vol. 4. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3432954
[262] Kuang Ming Kuo, Yu Chang Chen, Paul C. Talley, and Chi Hsien Huang. 2018. Continuance compliance of privacy policy of electronic medical records: the roles of both motivation and habit. *BMC Medical Informatics and Decision Making* 18, 1 (2018), 135. https://doi.org/10.1186/s12911-018-0722-7
[263] Sarah Kusumastuti, Heather Rosoff, and Richard S. John. 2019. Characterizing conflicting user values for cyber authentication using a virtual public values forum. *Decision Analysis* 16, 3 (2019), 157–171. https://doi.org/10.1287/deca.2018.0383
[264] Ari Kusyanti, Harin Puspa Ayu Catherina, and Yustiyana April Lia Sari. 2019. Protecting Facebook Password: Indonesian Users' Motivation. *Procedia Computer Science* 161 (2019), 1182–1190. https://doi.org/10.1016/j.procs.2019.11.231
[265] Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. 2020. Why do users not report spear phishing emails? *Telematics and Informatics* 48 (2020), 101343. https://doi.org/10.1016/j.tele.2020.101343
[266] Fujun Lai, Dahui Li, and Chang-Tseh Hsieh. 2012. Fighting identity theft: The coping perspective. *Decision Support Systems* 52, 2 (2012), 353–363. https://doi.org/10.1016/j.dss.2011.09.002
[267] Doohwang Lee and Robert LaRose. 2011. The Impact of Personalized Social Cues of Immediacy on Consumers' Information Disclosure: A Social Cognitive Approach. *Cyberpsychology Behavior and Social Networking* 14, 6 (2011), 337–343. https://doi.org/10.1089/cyber.2010.0069
[268] Hyun Hwa Lee and Jessica T. Hill. 2013. Moderating effect of privacy self-efficacy on location-based mobile marketing. *International Journal of Mobile Communications* 11, 4 (2013), 330. https://doi.org/10.1504/ijmc.2013.055747
[269] Jin-Myong Lee and Jong-Youn Rha. 2016. Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior* 63 (2016), 453–462. https://doi.org/10.1016/j.chb.2016.05.056
[270] Alex Leering, Lidwien van de Wijngaert, and Shahrokh Nikou. 2020. More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors. *Behaviour and Information Technology* 41 (2020), 1–16. Issue 3. https://doi.org/10.1080/0144929x.2020.1822444
[271] Rebecca LeFebvre. 2012. The Human Element in Cyber Security: A Study on Student Motivation to Act. In *Proceedings of the 2012 Information Security Curriculum Development Conference (InfoSecCD '12)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/2390317.2390318
[272] Ling Li, Wu He, Li Xu, Ash Ivan, Mohd Anwar, and Xiaohong Yuan. 2014. Does explicit information security policy affect employees' cyber security behavior? A pilot study. In *2014 Second International Conference on Enterprise Systems*. IEEE, Shanghai, China, 169–173. https://doi.org/10.1109/ES.2014.66
[273] Jiunn-Woei Lian. 2020. Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value. *Enterprise Information Systems* 15 (2020), 1–22. Issue 9. https://doi.org/10.1080/17517575.2020.1791966
[274] Cathy S. Lin. 2016. Educating Students' Privacy Decision Making through Information Ethics Curriculum. *Creative Education* 7, 1 (2016), 171–179. https://doi.org/10.4236/ce.2016.71017
[275] Chenhui Liu, Nengmin Wang, and Huigang Liang. 2020. Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management* 54 (2020), 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152
[276] Chen-Chung Ma, Kuang-Ming Kuo, and Judith W. Alexander. 2015. A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Medical Informatics and Decision Making* 16, 1 (2015), 13–23. https://doi.org/10.1186/s12911-016-0254-y
[277] Stanislav Mamonov and Marios Koufaris. 2016. The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security* 12, 2 (2016), 1–12. https://doi.org/10.1080/15536548.2016.1163026
[278] Debbie L. Manzano. 2012. *The cybercitizen dimension: A quantitative study using a threat avoidance perspective*. Vol. 73. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2013-99100-428&site=ehost-live
[279] Mohamad N. Masrek, Ismail Samadi, Qamarul Nazrin, and Atikah Azry. 2017. Modelling smartphone security behaviour of university students. *Turkish Online Journal of Educational Technology* 2, November Special Issue INTE (2017), 537–545. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057644658&partnerID=40&md5=87fd5560c3bb69d6bed94345d230df91
[280] Nik K.N. Mat, Yaty Sulaiman, and Selvan Perumal. 2019. Developing a New Model for Cyber Security Behavior of E-Hailing Services: A Conceptual Paper. In *2019 International Conference on Computer and Drone Applications (IConDA)*. IEEE, Kuching, Malaysia, 33–37. https://doi.org/10.1109/IConDA47345.2019.9034919
[281] Monica M. McGill, Sarah B. Lee, Litany Lineberry, John Sands, and Leigh Ann DeLyser. 2021. Piloting the Air Force JROTC Cyber Academy for High School Students. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21)*. Association for Computing Machinery, New York, NY, USA, 597–603. https://doi.org/10.1145/3408877.3432471
[282] Tanya McGill and Nik Thompson. 2017. Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour and Information Technology* 36, 11 (2017), 1–14. https://doi.org/10.1080/0144929x.2017.1352028
[283] Erica M. Mitchell. 2020. *Cyber security home: The effect of home user perceptions of personal security performance on household IoT security intentions*. Vol. 82. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-67315-129&site=ehost-live
[284] Norshidah Mohamed and Ili Hawa Ahmad. 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior* 28, 6 (2012), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

[285] Mohammadreza Mousavizadeh and Dan J. Kim. 2015. A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory. In *2015 International Conference on Information Systems: Exploring the Information Frontier*. AISeL, Fort Worth, TX, USA, 1–20.

[286] Florence Mwagwabi, Tanya McGill, and Mike Dixon. 2018. Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems* 42 (2018), 147–182. https://doi.org/10.17705/1CAIS.04207

[287] Quynh N. Nguyen and Dan J. Kim. 2017. Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. AISeL, Hilton Waikoloa Village, HI, USA, 4947–4956. https://doi.org/10.24251/hicss.2017.601

[288] Jacques Ophoff and Mcguigan Lakay (Eds.). 2019. *Mitigating the Ransomware Threat: A Protection Motivation Theory Approach*. Springer, Switzerland. https://doi.org/10.1007/978-3-030-11407-7{_}12

[289] Norman Pendegraft, Mark Rounds, and Robert W. Stone. 2010. Factors Influencing College Students' Use of Computer Security. *International Journal of Information Security and Privacy* 4, 3 (2010), 51–60. https://doi.org/10.4018/jisp.2010070104

[290] Hiep Cong Pham, Linda Brennan, and Steven Furnell. 2019. Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications* 46 (2019), 96–107. https://doi.org/10.1016/j.jisa.2019.03.012

[291] Vidia Poleon. 2020. *Millennials' information security habits and protection motivation intention: A quantitative study*. Vol. 82. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-67314-025&site=ehost-live

[292] Nirmalee I. Raddatz, Joshua G. Coyne, and Bradley S. Trinkle. 2020. Internal Motivators for the Protection of Organizational Data. *Journal of Information Systems* 34, 3 (2020), 199–211. https://doi.org/10.2308/isys-18-067

[293] Giulia Ranzini, Gemma Newlands, and Christoph Lutz. 2020. Sharenting, Peer Influence, and Privacy Concerns: A Study on the Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society* 6, 4 (2020), 1–13. https://doi.org/10.1177/2056305120978376

[294] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78. https://doi.org/10.1016/j.cose.2015.05.012

[295] Norsaremah Salleh, Ramlah Hussein, and Norshidah Mohamed. 2012. An Empirical Investigation on Internet Privacy on Social Network Sites among Malaysian Youths. *Journal of Information Technology Research* 5, 3 (2012), 85–97. https://doi.org/10.4018/jitr.2012070105

[296] Sushma Sanga. 2016. *The effect of electronic devices self-efficacy, electronic devices usage and information security awareness on identity-theft anxiety level*. Vol. 78. ProQuest LLC, Ann Arbor, MI, USA. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2017-23162-058&site=ehost-live

[297] Dilshani Sarathchandra, Kristin Haltinner, and Nicole Lichtenberg. 2016. College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. In *2016 Cybersecurity Symposium*. IEEE, Coeur d'Alene, ID, USA, 68–73.

[298] Michael Schade, Rico Piehler, Claudius Warwitz, and Christoph Burmann. 2018. Increasing consumers' intention to use location-based advertising. *Journal of Product & Brand Management* 27, 6 (2018), 661–669. https://doi.org/10.1108/jpbm-06-2017-1498

[299] Muliati Sedek, Rabiah Ahmad, and Nur Fadzilah Othman. 2018. Motivational Factors in Privacy Protection Behaviour Model for Social Networking. In *MATEC Web of Conferences*. EDP Sciences, Penang, Malaysia, 5 pages.

[300] Ahmad Bakhtiyari Shahri, Zuraini Ismail, and Shahram Mohanna. 2016. The Impact of the Security Competency on "Self-Efficacy in Information Security" for Effective Health Information Security in Iran. *Journal of Medical Systems* 40, 11 (2016), 241–249. https://doi.org/10.1007/s10916-016-0591-5

[301] Alexander T. Shappie, Charlotte A. Dawson, and Scott M. Debb. 2020. Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media* 9, 4 (2020), 475–480. https://doi.org/10.1037/ppm0000247

[302] Shavneet Sharma, Gurmeet Singh, Rashmini Sharma, Paul Jones, Sascha Kraus, and Yogesh K. Dwivedi. 2020. Digital Health Innovation: Exploring Adoption of COVID-19 Digital Contact Tracing Apps. *IEEE Transactions on Engineering Management* early access (2020), 1–17. https://doi.org/10.1109/TEM.2020.3019033

[303] Ming-Ling Sher, Paul C. Talley, Tain-Junn Cheng, and Kuang-Ming Kuo. 2017. How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Information Management Journal* 46, 2 (2017), 87–95. https://doi.org/10.1177/1833358316671264

[304] Ming-Ling Sher, Paul C. Talley, Ching-Wen Yang, and Kuang-Ming Kuo. 2017. Compliance With Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff. *INQUIRY The Journal of Health Care Organization Provision and Financing* 54 (2017), 1–12. https://doi.org/10.1177/0046958017711759

[305] Ruth Shillair, Shelia R. Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J. Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (2015), 199–207. https://doi.org/10.1016/j.chb.2015.01.046

[306] Ruth Shillair and William H. Dutton. 2016. Supporting a Cybersecurity Mindset: Getting Internet Users into the Cat and Mouse Game. In *Annual Meeting of the Telecommunications Policy Research Conference*. SSRN Electronic Journal, Arlington, VA, USA, 1–40.

[307] Jae-Hoon Shin and Sang-Hyun Choi. 2018. A study on personal information protection behavior in easy payment service: focused on protection motivation theory. *International Journal of Engineering and Technology* 7, 2.12 (2018), 132–135. https://doi.org/10.14419/ijet.v7i2.12.11108

[308] Mario Silic. 2017. Explaining Organizational Employee Computer Abuse Through an Extended Health Belief Model. *SSRN Electronic Journal* 24 (2017), 1–37. https://doi.org/10.2139/ssrn.3070823

[309] Mikko Siponen, M. Adam Mahmood, and Seppo Pahnila. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management* 51, 2 (2014), 217–224. https://doi.org/10.1016/j.im.2013.08.006

[310] Karen H. Smith, Francis A. Méndez Mediavilla, and Garry L. White. 2018. The Impact of Online Training on Facebook Privacy. *Journal of Computer Information Systems* 58, 3 (2018), 244–252. https://doi.org/10.1080/08874417.2016.1233001

[311] Siti N. Suhaimi, Nur F. Othman, Raihana Syahirah, Syarulnaziah Anawar, Zakiah Ayop, and Cik F.M. Foozy. 2020. Determinants of Privacy Protection Behavior in Social Networking Sites. *International Journal of Advanced Computer Science and Applications* 11, 12 (2020), 285–292. https://doi.org/10.14569/IJACSA.2020.0111236

[312] Zhenya Tang, Andrew S. Miller, Zhongyun Zhou, and Merrill Warkentin. 2021. Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly* 38 (2021), 101572. https://doi.org/10.1016/j.giq.2021.101572

[313] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security* 70 (2017), 376–391. https://doi.org/10.1016/j.cose.2017.07.003

[314] Ron Torten, Carmen Reaiche, and Stephen Boyle. 2018. The impact of security awarness on information technology professionals' behavior. *Computers & Security* 79 (2018), 68–79. https://doi.org/10.1016/j.cose.2018.08.007

[315] Bertrand Venard. 2019. The determinants of individual cyber security behaviours Qualitative research among French students. In *International Conference on Cyber Situational Awareness, Data Analytics And Assessment*. IEEE, Oxford, United Kingdom, 1–4.

[316] Silas Formunyuy Verkijika. 2018. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security* 77 (2018), 860–870. https://doi.org/10.1016/j.cose.2018.03.008

[317] Silas Formunyuy Verkijika. 2019. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior* 101 (2019), 286–296. https://doi.org/10.1016/j.chb.2019.07.034

[318] Silas Formunyuy Verkijika. 2020. Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. IEEE, Kimberley, South Africa, 1–13. https://doi.org/10.1109/IMITEC50163.2020.9334097

[319] Jeffrey D. Wall, Prashant Palvia, and Paul Benjamin Lowry. 2013. Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. *Journal of Information Privacy and Security* 9, 4 (2013), 52–79. https://doi.org/10.1080/15536548.2013.10845690

[320] Zhiqiang Wang and Yanjun Liu. 2014. Identifying key factors affecting information disclosure intention in online shopping. *International Journal of Smart Home* 8, 4 (2014), 47–58. https://doi.org/10.14257/ijsh.2014.8.4.05

[321] Jian M.C. Wee, Masooda Bashir, and Nasir Memon. 2016. Self-efficacy in cybersecurity tasks and its relationship with cybersecurity competition and work-related outcomes. In *2016 USENIX Workshop on Advances in Security Education*. USENIX Association, Austin, TX, USA, 1–8.

[322] Maor Weinberger, Dan Bouhnik, and Maayan Zhitomirsky-Geffet. 2017. Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior. *Open Information Science* 1, 1 (2017), 3–20. https://doi.org/10.1515/opis-2017-0002

[323] Maor Weinberger, Maayan Zhitomirsky-Geffet, and Dan Bouhnik. 2017. Factors affecting users' online privacy literacy among students in Israel. *Online Information Review* 41, 5 (2017), 655–671. https://doi.org/10.1108/oir-05-2016-0127

[324] Maor Weinberger, Maayan Zhitomirsky-Geffet, and Dan Bouhnik. 2017. Sex differences in attitudes towards online privacy and anonymity among Israeli students with different technical backgrounds. *Information research* 22, 4 (2017), 1–23. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039713647&partnerID=40&md5=8d4fb1f817bf19042b247763ccbb84b6

[325] Donghee Yvette Wohn and Chandan Sarkar. 2012. Expertise Matters: Privacy Perceptions and Practices in Response to Behavioral Targeting. *SSRN Electronic*

Journal 19 (2012), 1–30. https://doi.org/10.2139/ssrn.2046739

[326] Donghee Yvette Wohn, Jacob Solomon, Dan Sarkar, and Kami E. Vaniea. 2015. Factors Related to Privacy Concerns and Protection Behaviors Regarding Behavioral Advertising. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 1965–1970. https://doi.org/10.1145/2702613.2732722

[327] Chang-Gyu Yang and Hee-Jun Lee. 2016. A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers* 18, 2 (2016), 253–263. https://doi.org/10.1007/s10796-015-9594-x

[328] Chul W. Yoo, Jahyun Goo, and H. Raghav Rao. 2020. Is cybersecurity A team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly: Management Information Systems* 44, 2 (2020), 907–932. https://doi.org/10.25300/MISQ/2020/15477

[329] Chul Woo Yoo, G. Lawrence Sanders, and Robert P. Cerveny. 2018. Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems* 108 (2018), 107–118. https://doi.org/10.1016/j.dss.2018.02.009

[330] Cheolho Yoon, Jae-Won Hwang, and Rosemary Kim. 2012. Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education* 23, 4 (2012), 407–416. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84880826819&partnerID=40&md5=4a3c2d7fe5634802920874 1e54be814c

[331] Cheolho Yoon and Hyungon Kim. 2013. Understanding computer security behavioral intention in the workplace. *Information Technology and People* 26, 4 (2013), 401–419. https://doi.org/10.1108/itp-12-2012-0147

[332] F. Mariam Zahedi, Ahmed Abbasi, and Yan Chen. 2011. Design Elements that Promote the use of Fake Website Detection Tools. In *Tenth Annual Workshop on HCI Research in MIS*. arXiv, Ithaca, NY, USA, 1–5.

[333] Brahim Zarouali, Karolien Poels, Koen Ponnet, and Michel Walrave. 2018. "Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. *Cyberpsychology Journal of Psychosocial Research on Cyberspace* 12, 1 (2018), 1–19. https://doi.org/10.5817/cp2018-1-5

[334] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online Privacy Perceptions of Older Adults. In *Third International Conference (ITAP)*, Jia Zhou (Ed.). Springer International Publishing, Cham, Switzerland, 181–200. https://doi.org/10.1007/978-3-319-58536-9{_}16

[335] Jingzhi Zhang and Weiquan Wang (Eds.). 2018. *Effects of impulse and habit on privacy disclosure in social networking sites: Moderating role of privacy self-efficacy.* https://www.scopus.com/inward/record.uri?eid=2-s2.0-85089226353&partnerID=40&md5=0e353e39779272b20b79f44c2dde8111

[336] Xing Zhang, Shan Liu, Xing Chen, Lin Wang, Baojun Gao, and Qing Zhu. 2018. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management* 55, 4 (2018), 482–493. https://doi.org/10.1016/j.im.2017.11.003

[337] Jie Zhen, Zongxiao Xie, and Kunxiang Dong. 2020. Positive emotions and employees' protection-motivated behaviours: a moderated mediation model. *Journal of Business Economics and Management* 21, 5 (2020), 1466–1485. https://doi.org/10.3846/jbem.2020.13169

[338] Guangyu Zhou, Mengke Gou, Yiqun Gan, and Ralf Schwarzer. 2020. Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage. *Frontiers in Psychology* 11 (2020), 1066. https://doi.org/10.3389/fpsyg.2020.01066

[339] Xingzhen Zhu, Peng Zhu, and Yanmei Qiu. 2018. Research on the Influence of Fear Appeals on APP Users' Privacy Protection Behavior. In *Proceedings of the 2018 International Conference on Information Management & Management Science (IMMS '18)*. Association for Computing Machinery, New York, NY, USA, 200–205. https://doi.org/10.1145/3277139.3277172

Table A1: Results for Separate Analysis of Peer-Reviewed and Non-Peer-Reviewed Publications

	Peer-Reviewed	Non-Peer-Reviewed
Number of publications	131	19
Median sample size	$MD = 290$	$MD = 188$
Sample size range	12 to 1663	20 to 569
Number of scales	129	25
Number of first use scales	122	21
Weighted mean alpha of first use scales	$M = 0.87$ ($SD = 0.06$)	$M = 0.85$ ($SD = 0.06$)
Number of first use scales reporting validity	90	15
Number of cause variables	76	12
Number of outcome variables	138	25
Number of cause-and-outcome variables	8	–
Number of interventions	7	4

Note. Data from publications that did not provide information about the review process ($N = 18$) was not included in this exploratory analysis.

Table B1: Summary of Criteria Reported with Respect to the Methodological Rigor of First Use Measures

Ref.	Scale	Definition	Items	Facets	Reliability				Validity							
					α	CR	Test-Retest	Splithalf	Content	Experts	Factor	Fitindices	Discriminant	Convergent	Criterion	Incremental
[227]	1	1	1	0	0	1	0	0	0	0	0	0	1	1	0	0
[173]	2	1	1	0	0	0	0	0	1	1	0	0	1	0	0	0
[176]	3	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[177]	4	1	1	0	0	1	0	0	1	1	0	0	0	0	0	0
[178]	5	1	1	0	1	0	0	0	1	1	0	0	1	1	0	0
[186]	7	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
[191]	8	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[195]	9	1	0	0	0	0	0	0	1	0	0	0	1	1	0	0
[199]	11	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
[201]	12A	1	1	0	0	1	0	0	1	1	1	0	1	1	0	0
[218]	12B	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[188]	12C	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[188]	12D	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[188]	12E	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[188]	12F	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[329]	12G	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0
[260]	12H	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[275]	12I	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[203]	13	1	1	1	1	0	0	0	1	0	1	0	0	0	0	0
[209]	14	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[215]	15	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[216]	16	1	1	0	1	0	0	0	1	0	1	0	1	1	0	0
[219]	18	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[232]	21	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[233]	22	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
[235]	24	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[236]	25	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[242]	26	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[243]	27	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[245]	28	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[248]	29	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
[253]	30	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[262]	31	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[266]	33A	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[320]	33B	1	1	0	1	0	0	0	0	0	0	0	1	1	0	0
[267]	34	0	1	0	1	0	0	0	0	0	0	0	1	1	0	0
[270]	35	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[271]	36	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[271]	37	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[271]	38	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[277]	39	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[283]	40	1	1	0	1	0	0	0	1	0	0	0	1	1	0	0
[280]	41	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
[294]	43	1	1	0	0	1	0	0	1	0	0	0	1	1	0	0
[295]	44	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0
[296]	45	1	1	0	1	0	0	0	1	1	0	0	1	1	0	0

Note. 1: information about the criterion was reported; 0: information about the criterion was not reported; α: coefficient alpha; CR: composite reliability.

Table B1 Cont. Summary of Criteria Reported with Respect to the Methodological Rigor of First Use Measures

Ref.	Scale	Definition	Items	Facets	Reliability				Validity							
					α	CR	Test-Retest	Splithalf	Content	Experts	Factor	Fitindices	Discriminant	Convergent	Criterion	Incremental
[297]	46	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[268]	47A	1	1	0	1	0	0	0	0	0	0	0	1	1	0	0
[298]	47B	1	1	0	1	1	0	0	1	0	1	0	1	1	0	0
[300]	48	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
[304]	49	1	1	0	0	1	0	0	1	0	0	0	1	1	0	0
[308]	50	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0
[309]	51	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[332]	52	1	0	0	0	0	0	0	1	0	0	0	1	1	0	0
[339]	53	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0
[184]	54	1	1	0	0	1	0	0	1	1	0	0	0	0	0	0
[174]	55	0	1	0	1	1	0	0	1	0	0	0	1	0	0	0
[179]	56	0	1	0	1	0	0	0	1	1	0	0	1	1	0	0
[183]	57	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0
[229]	58	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
[194]	59	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0
[197]	61A	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[197]	61B	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[197]	61C	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[202]	62	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[205]	63	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[206]	64A	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[206]	64B	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[207]	65	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[211]	66	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[212]	67	1	1	0	1	0	0	0	1	1	0	0	1	1	0	0
[214]	68	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[223]	69	0	1	1	1	1	0	0	0	0	0	0	0	1	0	0
[224]	70	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[282]	71A	0	1	0	1	0	0	0	1	1	0	0	0	0	0	0
[226]	71B	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[228]	72	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
[237]	73	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[239]	74	0	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[241]	75	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[244]	76	1	0	0	1	0	0	0	1	1	0	0	0	0	0	0
[247]	77	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[175]	78	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
[251]	79	1	0	0	0	1	0	0	1	1	0	0	1	1	0	0
[255]	80	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0
[257]	81	1	1	0	1	0	0	0	1	0	0	0	1	1	0	0
[258]	82	0	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[269]	83	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0
[250]	85A	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[288]	85B	0	1	0	0	1	0	0	1	0	0	0	1	1	0	0
[289]	86	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[290]	87	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0
[291]	88	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0

Note. 1: information about the criterion was reported; 0: information about the criterion was not reported; α: coefficient alpha; CR: composite reliability.

Table B1 Cont. Summary of Criteria Reported with Respect to the Methodological Rigor of First Use Measures

Ref.	Scale	Definition	Items	Facets	Reliability				Validity							
					α	CR	Test-Retest	Splithalf	Content	Experts	Factor	Fitindices	Discriminant	Convergent	Criterion	Incremental
[284]	89A	1	1	0	0	1	0	0	0	0	0	0	1	1	0	0
[318]	90	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0
[301]	91	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[303]	92	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[305].	93	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[306]	94	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0
[312]	95	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[316]	96	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[319]	97	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[323]	98	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[325]	99	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[326]	100	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[328]	101	0	1	0	1	1	0	0	1	1	1	1	1	1	0	0
[330]	102	1	1	0	0	1	0	0	0	0	0	0	1	1	0	0
[335]	103	1	0	0	0	1	0	0	1	1	0	0	1	1	0	0
[336]	104	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[337]	105	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[172]	106	1	0	0	1	0	0	0	1	0	0	0	1	1	0	0
[180]	107	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0
[181]	108	1	1	0	1	0	0	0	1	1	0	0	0	0	0	0
[187]	109	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0
[187]	110	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0
[190]	111	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[192]	112	1	1	1	1	0	0	0	1	0	1	1	1	1	0	0
[193]	113	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[200]	114	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[208].	115	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
[210]	116	1	1	0	1	0	0	0	0	0	0	0	1	1	0	0
[321]	117	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0
[221]	118	1	0	0	0	0	0	0	1	0	0	0	1	1	0	0
[222]	119A	0	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[222]	119B	0	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[222]	119C	0	1	0	0	1	0	0	1	0	0	0	1	1	0	0
[225]	120	1	1	0	1	0	0	0	1	1	0	0	1	1	0	0
[238]	121	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0
[240]	122	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[307]	123	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0
[249]	124	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0
[252]	125	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[254]	126	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[256]	127	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0
[259]	128	0	0	0	0	1	0	0	1	1	1	0	1	1	0	0
[261]	129	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[263]	130	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
[264]	131	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
[265]	132	1	1	1	1	0	0	0	1	0	1	1	0	0	0	0
[272]	133	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0

Note. 1: information about the criterion was reported; 0: information about the criterion was not reported; α: coefficient alpha; CR: composite reliability.

Table B1 Cont. Summary of Criteria Reported with Respect to the Methodological Rigor of First Use Measures

Ref.	Scale	Definition	Items	Facets	Reliability				Validity							
					α	CR	Test-Retest	Splithalf	Content	Experts	Factor	Fitindices	Discriminant	Convergent	Criterion	Incremental
[273]	134	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
[274]	135	1	1	1	0	1	0	0	0	0	1	0	1	1	0	0
[276]	136	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0
[278]	137	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[279]	138	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
[285]	139	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[286]	140	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[246]	141	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0
[287]	142	1	0	0	1	1	0	0	0	0	0	0	0	1	0	0
[213]	143	1	1	0	0	0	0	0	1	0	0	0	1	1	0	0
[292]	144	1	0	0	1	1	0	0	1	0	0	0	1	1	0	0
[230]	145	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[299]	146	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0
[311]	148	1	0	0	1	0	0	0	1	1	0	0	1	1	0	0
[315]	149	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0
[317]	150	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[327]	151	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0
[331]	152	0	1	0	0	1	0	0	1	0	0	0	1	1	0	0
[333]	153	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
[334]	154	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0
[338]	155	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0

Note. 1: information about the criterion was reported; 0: information about the criterion was not reported; α: coefficient alpha; CR: composite reliability.

Table B2: Summary of Criteria Reported with Respect to the Methodological Rigor of Recurring Measures

Ref.	Scale	Definition	Items	Facets	Reliability				Validity							
					α	CR	Test-Retest	Splithalf	Content	Experts	Factor	Fitindices	Discriminant	Convergent	Criterion	Incremental
[182]	6	1	1	0	1	0	0	0	1	0	0	0	1	1	0	0
[198]	10	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
[204]	13	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0
[217]	17	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0
[220]	19	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0
[231]	20	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0
[234]	23	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
[185]	32	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0
[189]	42	1	0	0	0	1	0	0	1	0	0	0	1	1	0	0
[196]	60	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0
[313]	71A	0	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[314]	74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[281]	84	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
[293]	89B	1	1	0	1	1	0	0	0	0	1	0	1	0	0	0
[324]	98	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[322]	98	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
[302]	104	1	1	0	1	1	0	0	1	0	0	0	1	1	0	0
[310]	147	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0

Note. 1: information about the criterion was reported; 0: information about the criterion was not reported; α: coefficient alpha; CR: composite reliability.

Table C1: Results for Separate Analysis of Newly Created and Adapted Measures

	Newly Created	Adapted
Number of measures	49	112
Number of studies	49	107
Number of studies reporting reliability information[1]	29	94
Number of studies reporting...		
alpha coefficient	25	77
composite reliability	12	64
two out of four reliability estimates	8	39
Weighted mean alpha	$M = 0.873$ ($SD = 0.060$)	$M = 0.862$ ($SD = 0.062$)
Weighted mean composite	$M = 0.888$ ($SD = 0.048$)	$M = 0.905$ ($SD = 0.057$)
Number of studies reporting validity information[1]	26	91
Number of studies reporting...		
content validity	18	68
factor validity	3	8
discriminant validity	17	79
convergent validity	18	75
criterion validity	–	1
two out of six validity types	6	25
three out of six validity types	9	47
four out of six validity types	2	5
Number of discriminant and convergent validity constructs	64	258
Number of excl. discriminant validity constructs	4	11
Number of excl. convergent validity constructs	15	6

Note. This exploratory analysis divides the outcomes reported in the results section for first use scales into newly created and adapted scales; [1]One study may report multiple estimates or types.

Table D1: Cause Variables of Cybersecurity Self-Efficacy

Frequency	Cause
10	awareness
7	expertise, gender
6	experience, training
5	positive emotions
4	age, negative emotions
3	information security policy, knowledge, support
2	awareness campaign, concerns, control salience, education, habit, learner control and feedback, literacy, norms, perceived risk, threat severity, threat susceptibility, vicarious experience
1	agreeableness, attitude, avoidance behavior, competition effectiveness for recruitment, competition performance and satisfaction, conscientiousness, culture, device type, dominant orientation, ease of use, effort, extroversion, fatigue, gaming, government social media participation, hearsay, innovativeness, interest, job satisfaction, learner engagement, loss, mental resources, monitoring and evaluation, neuroticism, news exposure, openness, organizational climate, organizational fit, peer influence, problematic behavior, protection behavior, psychological reactance, reading information, response efficacy, rewards, sanctions, self-determination, self-technical controllability, serenity, sharing, shyness, surprise, system satisfaction, training effectiveness, usefulness, verbal persuasion, work arrangement

Table D2: Outcome Variables of Cybersecurity Self-Efficacy

Frequency	Outcome
25	security behavior
19	compliance intention
17	security intention
11	concerns
10	protection intention
7	compliance behavior, protection behavior
6	avoidance motivation, outcome expectation
5	behavioral control, disclosure behavior, disclosure intention
4	coping, use behavior
3	attitude, awareness, expertise, friending, information security problem, perceived threat, privacy behavior, profile visibility, protection motivation
2	avoidance intention, behavioral intention, collective efficacy, perceived risk, risky behavior, security effectiveness, sharing willingness
1	adoption intention, advertisement persuasiveness, anxiety, approach intention, assurance behavior, avoidance behavior, competition effectiveness for recruitment, competition performance and satisfaction, compliance habit, consumer typology, coordination, critical processing, danger control, effort, fear control, hearsay, interest, job satisfaction, literacy, organizational fit, password metrics, perceived control, perceived importance, perceived protection, perceived value, policy deviation decision, privacy empowerment, privacy intention, privacy management strategies, problematic behavior, reinforcement intention, reporting, response cost, response efficacy, security perceptions, self-monitoring, self-regulation, sharenting, sharing, system satisfaction, trust beliefs, trust intention, use intention, victimization

Table D3: Cause-and-Outcome Variables of Cybersecurity Self-Efficacy

Frequency	Cause-and-Outcome
13	awareness, concerns
10	expertise
8	protection behavior
4	attitude, perceived risk
3	literacy
2	avoidance behavior, competition effectiveness for recruitment, competition performance and satisfaction, effort, hearsay, interest, job satisfaction, organizational fit, problematic behavior, response efficacy, sharing, system satisfaction