Birlesik Dünya Arastırma BD CENTER Innovasyon ve Yayıncılık Merkezi

Cypriot Journal of Educational Sciences

Volume 15, Issue 5, (2020) 955-975

CJES Cypriot Journal of Educational Sciences

www.cjes.eu

Insights on media literacy and social engineering vulnerability predictors: Lifelong learning gravity

Michelle Adi Nugraha [a], Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia https://orcid.org/0000-0002-2177-1360
Nadhia Prili Banglali [b], Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia https://orcid.org/0000-0001-8214-7687
Juneman Abraham [c*], Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia https://orcid.org/0000-0003-0232-2735
Moondore Madalina Ali [d], Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia https://orcid.org/0000-0002-1642-7514
Esther Widhi Andangsari [e], Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia https://orcid.org/0000-0002-0073-5985

Suggested Citation:
Nugraha, M. A., Banglali, N. P., Abraham, J., Ali, M. M., & Andangsari, E. W. (2020). Insights on media literacy and social engineering vulnerability predictors: Lifelong learning gravity. *Cypriot Journal of Educational Science*. *15*(5), 955-975. https://doi.org/10.18844/cjes.v15i5.5124

Received from June 10, 2020; revised from August 12, 2020 ; accepted from October 15, 2020.
Selection and peer review under responsibility of Prof. Dr. Huseyin Uzunboylu, Higher Education Planning, Supervision, Accreditation and Coordination Board, Cyprus.

Abstract

Effective learning in the current 4.0 Industrial Revolution era may not happen if a learner is insensitive to two types of social engineering, namely phishing and tailgating. This study aims at investigating the predictors of vulnerability to phishing and tailgating from the psychological perspective. The study was conducted on a sample of Indonesians (125 males, 137 females; M_{age} = 28 years old, SD_{age} = 8.319 years); considered as the 'millennial' age group. Multiple linear regression analyses covering seven predictors of the vulnerabilities, i.e. insufficient knowledge/media literacy, excitement of victory, fear of authority, desire to be helpful, fear of loss, laziness, and appeal to ego, showed that the psychological models predicting vulnerability of experiencing phishing and tailgating were confirmed, with an effect size range between 18.5% to 19%. Media literacy alone was proven to be inadequate in managing/deterring the variables that embrace vulnerability to the two social engineering techniques. The relevance of this study to lifelong learning gravity is discussed throughout this article.

Keywords: lifelong learning; literacy; phishing; psychological vulnerability; social engineering; tailgating

* ADDRESS FOR CORRESPONDENCE: Juneman Abraham, Psychology Department, Faculty of Humanities, Bina Nusantara University, Jl. Kemanggisan Ilir III/45, DKI Jakarta 11480, Indonesia
E-mail address: juneman@binus.ac.id / Tel.: +62-21-534-5830 ext. 2632

1. Introduction

The world of education, especially during the Covid-19 pandemic, increasingly relies on digital learning. Nevertheless, learning and training activities among high school students, university students, as well as corporate employees are never separated from other online activities, such as browsing general sites for information searches, and enjoying entertainment (as a leisurely distraction between study or work periods). Aldawood and Skinner (2019) stated that social engineering awareness training is a valuable investment in every educational organization, and there is a need to (1) build a profile of learners who are "at-risk", as well as (2) keep the organization alert to the development and risk of social engineering amongst the organization's constituents. The training of social engineering literacy has a cost-efficiency benefit because protection against phishing and tailgating attacks will exhaust an organization's financial resources if it only relies on upgrading physical and electronic infrastructures. Thus, the psycho-educational and literacy aspects that require improvements become an emphasis in this present study.

It is not surprising that literacy on digital and cyber security has become an essential part of a lifelong learning curriculum, such as the *Lifelong-learning.lu* portal by the National Institute for The Development of Continuing Vocational Training (INFPC, 2020). Continuous education on digital security literacy is critically needed by educational institutions or corporations, particularly due to the fact that "cyber security challenges are continuously developing due to hackers' forever changing tactics, techniques and technologies" (Smith, 2018, p. 6). In fact, the gamification presented by social media carries the risk of phishing (Edwards, 2014). Tasevski (2016) suggested interdisciplinary-based education and training to address security issues, as recent issues require not only anticipatory awareness and literacy, but also contextual culture, history, and globalization consciousness. For further implications, cyber security training must involve "social partnership between higher educational institutions, the state, business, domestic and international or public organizations" (Voskoboinicov & Melnyk, 2018, p. 109-110). Here lies the importance of the present study, as it contributes from psychological discipline by recruiting research participants from professional and business settings, as they may offer insights on how socio-organizational resources are spent or can be protected in the scope of cyber crime, media literacy, individuals' vulnerability, and social engineering.

Two major campuses in Indonesia, namely the University of Indonesia (UI) and the State Islamic University of Maulana Malik Ibrahim Malang (UIN Malang), recently reported electronic hacking (Hartik, 2020; Ramadhanny, 2020). The hacked website at UI is a medical faculty research site (Medical Education Unit/MRU subdomain) and a computer science faculty website. Information about data leaks at UI came from the National Cyber Security Operations Center of the National Cyber and Code Agency. Whereas at UIN Malang, the hacking of Zoom was colored by vandalism when the Vice President of the Republic of Indonesia was delivering his educational speech on Sharia Economics to the academicians. Events such as these have the potential of lowering the public's trust on academic institutions as their ability in dealing with hacking, as one of the entrances to phishing, is viewed as inadequate.

Technology disruption impacts not only acceptance and competence in using technological solutions (such as mobile applications), as well as mental restructuring, but also readiness in facing security issues from both of the realities, online, i.e. phishing, and offline, i.e. tailgating. These social engineering techniques are intended by the perpetrators as a means to steal the credentials of the institution's personnel, in order to obtain financial benefits and destroy the institution's reputation or dismantle security for other purposes.

As the technological era develops, criminal acts such as fraudulence have a variety of forms. From face-to-face frauds to digital-based frauds where information and communication technology (ICT) systems augment the variety of technological crimes. When such systems are applied, there is usually an in increased risk for fraud to occur. For example, a victim was promised by a fraud schemer to be given an "appreciation as a *so-called* '*Gojek*' (Indonesian online-based-booking motorcycle taxi) customer" with a large amount of money, i.e. 1.5 million rupiahs (104.73 USD), in the form of electronic money (so-called *GoPay*) with several procedures to be followed through as a requirement to receive the money (Rachmatunnisa, 2018). The instructions of the procedure were given through telephone by requesting an OTP (One Time Password) code sent via SMS so that the perpetrator has access to the victim's mobile app (Pertiwi, 2019), and consequently, this usually ends in the extraction or withdrawal of the victim's available electronic money within the app. This phenomenon of online fraud is very common, and many groups, such as private companies, Government bodies, education institutions, and mass media organizations, have exerted efforts to reduce and prevent this trend. Due to this trend, Indonesia was considered the riskiest country to experience an attack on technological security and was ranked at the top with a 23.54% risk for the general public of being attacked (SophosLabs's Security Threat Report, as cited in Proxsis Consulting Group, 2020).

The phenomenon does not only occur through telephone but also through various platforms such as websites and emails, in which fraudulent profiles are designed similarly to original and legitimate businesses, government financial institutions to deceive internet users so that users may leak their personal information. The attackers falsify their identity and claim themselves as representatives or officials of a legitimate institution in order to deceive victims and steal their personal information; this is known as "phishing" (Shetty, 2011). Additionally, other forms of online fraud in Indonesia occur through online shopping, online loans, *WhatsApp* hijacking, to electronic money frauds (Alfarizi, 2019).

The techniques that perpetrators benefit from victims' lack of media literacy have had significant successes as seen from the high number of financial loss due to frauds that have occurred in Indonesia, up to 36 billion rupiahs (2,513,466 USD) in 2019 (Halim, 2019; Marhaenjati, 2019). In this context, media literacy "represents the essential competencies that equip the citizens with abilities to effectively engage with the media and develop critical thinking and lifelong learning skills to socialize and become active citizens" (UNESCO, as cited in Alshorooqi & Rawadieh, 2017, p. 261).

However, fraud is not only based on the ability of fraudsters in achieving their success to deceive; and not all frauds are carried out successfully by the plans of fraud schemers. Various technological efforts, such as improving security in the form of firewalls, investigating the development phase of the available software's life cycle, encouraging awareness or literacy of information security in the world of ICT, are not enough to handle hacking threats (Kavanagh, 2019; Rafique et al., 2015; Safianu, Twum, & Hayfron-Acquah, 2016). Factors from both parties, fraud schemers and their targets, influence the success of committed fraud. Aside from these factors, threats do not only come from hackers but may also come from nature: such as natural disasters that damage hardware and direct exposure from attackers who destroy the hardware itself (Abomhara & Køien, 2015).

This article will discuss the phenomena and the factors that influence the success of fraud **from a victim's perspective**. This is because efforts such as training in the literacy of fraud provided by many media/ICT expert groups have been carried out but yielded minimal success (Vielberth, Menges & Pernul, 2019). It is urgent to empower the masses in terms of their behavior and knowledge on safety precautions, and actively increase their organization's confidence or wider community's safety, as well

as to avoid threats of fraud that result in waste and abuse of personal or organizational resources (Heartfield, Loukas, & Gan, 2017; Safianu et al., 2016).

1.1. Phishing and Tailgating: Two Forms of Social Engineering

Social engineering crimes are done by manipulating victims and making victims believe a scheme until they provide hackers access to their technology accounts or platforms. **Social engineering** is a form of manipulative attack that allows hackers to gain control of a person's confidential information by exploiting his/her habits, motivations, and cognitive biases; a psychological manipulation designed to influence social behavior and trustworthiness; a mental manipulation to deceive computer users so hackers can access the victim's personal computer and take it over (Abass, 2018; Fahey, 2016; Goel, Williams & Dincelli, 2017).

There are several techniques of social engineering, i.e. phishing, spear phishing, baiting, scareware, pretexting, watering hole attack, and quid pro quo (Bansla, Kunwar, & Gupta, 2019; Lohani, 2019). Thapar (2007), divided the techniques into 2 vectors, i.e. technical (include phishing, vishing, pop-up windows, interesting software, and spam emails) and non-technical (hoaxing, pretexting, dumpster diving, spying, authoritative voice, support staff and acting as a technical expert). From several **technical techniques**, *phishing* is one of the most performed social engineering techniques.

Phishing is a technique that uses emails and written messages that aim to increase the seriousness, importance, strangeness, or generate a panic impression on a target or victim (Bansla, et al., 2019). These techniques are used to convince the target that the sender is a legitimate business, bank, or credit card company that asks for "verification" of personal information and forewarn the terrible consequences if not followed through (Thapar, 2007; Abass, 2018), and usually in the sent email, the perpetrator includes a link that directs the victim to a dangerous artificial website (Lohani, 2019). Techniques used in phishing encompass use of legitimate links; mixing legitimate and dangerous codes; abuse of URL redirects and shortenings; blurring brand logos; and confusing filters with less content or excessive noise (Basset, 2019). The attackers manipulate the target by inducing a sense of alignment with their goals that further causes them to be less careful in dealing with the attackers (Abass, 2018). From these examples, it is evident that techniques of social engineering attack people's feelings and play with their unconscientiousness.

Tailgating, or also known as piggybacking, is one of the social engineering types that is slightly different from other types because this technique requires attackers to exclusively and physically interact with the target (SecurityTrails, 2020). This type of attack involves perpetrators requesting access to a physically restricted area or space, or a digital organization. A common reported scenario in organizational settings is that attackers ask employees to "hold the door" to a restricted area because they forgot their access or identity cards, or to ask employees to borrow a tool that they do not have. This attack will be very useful in large organizations where the employees do not recognize their co-workers, so the targets are often easily deceived. A person without proper authentication follows the employee who is authenticated to the restricted area; the attacker might impersonate a delivery driver and wait outside the building, and when an employee gets a security agreement and opens the door, the attacker asks the employee to hold the door, thus gaining access to the building (Bisson, 2019). Tailgating does not always work across all organizational settings such as large companies that need access cards for entrance. However, in medium-sized or low-security companies, attackers can simply start to have conversations with the employees and use a display of intimacy to pass the receptionist and enter the company's premises (Bisson, 2019).

1.2. Psychological Vulnerability: Its Dimensions and Predictors

Psychological vulnerability refers to the cognitive structures that cause an individual's susceptibility to stress; a pattern of cognitive beliefs that reflect a dependence on achievement or an external source of affirmation upon one's self-esteem (Sinclair & Wallston, 1999; Sinclair & Wallston, 2010). This kind of vulnerability involves many individual and group characteristics that cause them to feel threatened and limit their ability to anticipate, overcome, and recover from danger (Wisner, 2016).

There are three vulnerability dimensions (Wisner, 2016). *First*, **exposure**, which is the characteristics and the extent (in terms of frequency, duration, and area of danger) to which someone experiences pressure in the environment. *Second*, **susceptibility**, which is the extent to which individuals or groups suffer from the processes or factors that threaten them in the event of an exposure. *Third*, **coping and adaptation capacity**, which is the ability of individuals or groups in using the skills and available resources to manage adverse situations, risks, or disasters; to adapt to changing situations that can cause potential damage, take advantage of opportunities, or overcome the consequences.

Some human psychological factors are vulnerable to social engineering (see Table 1); however, there are no quantitative psychological studies investigating them in an integrated manner (including Pîrnau, 2017).

Table 1. The predictors of psychological vulnerability

Thapar (2007)	**Shetty (2011)**
Enthusiasm to get free rewards	Excitement of victory
Appeal to authority	Fear of the authority
Desire to be helpful	Desire to be helpful
Fear of losing-incurring a loss	Fear of loss
Laziness	Laziness
Appeal to ego	Ego
Low perceived cost of information	Insufficient knowledge

The brief explanation about the concepts mentioned in Table 1 is as follows: People who are **susceptible in becoming victims of social engineering** are, among others, people who are **excited or enthusiastic** about a situation where they could win meaningful prizes (Shetty, 2011). While **fear of the authority** or appeal to authority is the reason for the authoritative voice technique (utilizing credential information of certain parties to convince targets that requests from schemers are very feasible to be fulfilled) was successful (Thapar, 2007). The victim or target is predetermined as possessing a tendency to fear and obey authority (Shetty, 2011). Lastly, the targets of social engineering who wish to help others–i.e. has the **desire to be helpful** in terms of involvement in social relationships, the inclination of a person and a human's natural tendency to help and to be liked–are likely to provide information that should not be disclosed to strangers as it allows

perpetrators to gain unauthorized access to the targeted system that is likely to cause potential losses (Abass, 2018; Shetty, 2011). The desire to win offered prizes, e.g. something that is rarely owned by others, increases when the feeling of the ability to own that offer decreases in the future (Abass, 2018).

The desire to win rewards also causes victims to end in a 'phishing trap', which can be in the form of an email that is sent to the victims, notifying them that they have won a sum of money and if they do not respond to that email (by following directions to send a sum of money to a designated account in order to receive the reward in return), the prize would be rolled to the next "winner". Whereas when someone faces **fear of loss,** including loss of profits that cause victims to fear missing out on a good opportunity, and that they will have no second chances in the future, they are coerced to respond to such "advantageous" opportunities with limited time—by not making deliberate considerations, or acting directly with utter confidence and consequently fall into a fraud scheme (Rigby, 2019; Shetty, 2011).

Laziness is described as a human tendency to be bored with habits and attempts to find a shortcut to achieve something, and this tendency is one out of many human behaviors that is frequently targeted by attackers (Shetty, 2011). **Ego** or **appeal to ego** (**i.e. self-importance)** is a framework that is embedded in humans where individuals tend to succumb to their emotional ego when they are presented with an exciting stimulus, without thinking logically. The attacker will make a scenario to which the target gives in to his/her emotional side and abandon logical thinking (Shetty, 2011). The attacker also targets someone who has **insufficient knowledge/literacy** about the real and legitimate institution or company. This is used for the attacker to commit fraud without any suspicion from the victim or target who (Shetty, 2011).

1.3. Hypotheses

This present study aims to test the hypotheses that:

- There are psychological models predicting the vulnerability of experiencing phishing (H1) and tailgating (H2).
- The excitement of victory (H3), fear of the authority (H4), desire to be helpful (H5), fear of loss (H6), laziness (H7), ego (H8), and insufficient knowledge/literacy (H9) can predict the vulnerability of experiencing phishing.
- The excitement of victory (H10), fear of the authority (H11), desire to be helpful (H12), fear of loss (H13), laziness (H14), ego (H15), and insufficient knowledge/literacy (H16) can predict the vulnerability of experiencing tailgating.

2. Methods

2.1. Sample and Data Collection

The participants of this research were 262 people with an age range of 19 years to 56 years (125 males, 137 females, M_{age} = 28 years old, SD_{age} = 8.319 years) and were predominantly of Javanese ethnicity with a total of 109 respondents (42%), followed by Betawis (6%) and Batak (9%), Sundanese (7%) and another combination of other ethnic groups (26%). Participants were mostly undergraduates / held undergraduate degrees (54%), senior high students / held senior high degrees (30%), diploma students / held diploma degrees (11%), postgraduate students/ held postgraduate degrees (4%) and

junior high school students/ held junior high school degrees (1%) of the total. The samples were collected through a non-probabilistic, convenience sampling method.

Informed consents were obtained from the participants with brief information about the research purpose, procedure, protection of confidentiality, their rights to withdraw, as well as the potential publication of the study results.

The **demographic data** collected from the participants consisted of a distinctive age range, e.g. early adulthood (considered an age group whereby people enter numerous transitions including environmental, social and lifestyle changes) that represents life-altering factors, according to Erik Erikson (as cited in Lumen, n.d.), such as working, romantic relationships and connectedness (Winpenny et al., 2018). Furthermore, length of work service was identified, assuming that the more time spent in one job, the more knowledge about the job is acquired. The questionnaire also consisted of a statement on the importance of privacy.

2.2. Instruments

From the perspective of lifelong learning, emotions, cognitions, behavior and personality that are correlated with a person's vulnerability to social engineering "can all be learnt". As an example, Hammond (2004) discovered that lifelong learning is able to shape emotional resilience in a positive way. In addition, Regmi (2020) also highlighted the importance of the combination between a psychological and social approach in lifelong learning, in order to generate "interactive competence" (p. 13), that is, a competence to participate in communication processes. In the context of this study, such competence is deemed vital for an individual to deal with phishing and tailgating, and other psychological capacities are also integral to it, including managing emotions (fear, excitement, etc.), cognitions (media literacy), behavior (laziness), and personality (ego).

To measure **the dependent/criterion variables**, i.e. **vulnerability to phishing** and **vulnerability to tailgating**, the Indonesian-language scales used were derived from the dimensions formulated by Wisner (2016) consisting of (1) exposure, (2) susceptibility, and (3) coping and adaptation capacity. The items are presented in the Table 2.

Table 2. The study's psychological scales

Variable	Dimension	Indicator	Item
Vulnerability to Phishing (DV 1)	Exposure (α = 0.810)	Exposure with emails from strangers	I often receive emails from people I don't know.
		The number of emails that come in every day	Within 1 day I usually receive more than five.
			Within 1 day I will receive at least 1 e-mail from an unknown source (unknown person or organization).
		Number of emails received	I tend to receive email requests of various types (Example: downloading files, verifying personal data).

Variable	Dimension	Indicator	Item
			I often get emails containing websites with fake domain names (Example: T0koPedya, instead of Tokopedia).
	Susceptibility (α = 0.639)	Does not install security devices or Antivirus	I do not install security devices on my computer (Example: Antivirus, Firewall).
		Forgets to logout	I often forget to log out from my email or social media on my computer.
			I often forget to log off my computer when I want to leave my workspace.
		Gets lured by E-mails	Some of the emails that come in often state that I won a lottery (Example: some money or free vacation).
	Coping and adaptation capacity (α = 0.664)	Avoid downloading files from untrusted web addresses	I tend not to download files from emails or websites that I don't know about if I'm asked to download a file.*
		Being able to distinguish the types of incoming email	I can distinguish the types of emails that come in.*
		Able to avoid unnecessary requests for information	I will not give information to sources I don't know about.*
		The ability to deal with people who threaten the security of personal data	I am able to improve/manage the security data that is on my computer.*
		The ability to follow-up	I will report to the authorities if I get an email or call from someone who asks for information that is not reasonable.*
			I will take my computer to a computer expert to get rid of the viruses that are on my computer.*
Vulnerability to Tailgating (DV 2)	Exposure (α = 0.642)	Many and varied guests	I often meet people who know me but I don't know them.
			I often meet people who make me

Variable	Dimension	Indicator	Item
			feel reluctant not to fulfill their requests.
	Susceptibility (α = 0.611)	Forgot to logout	I often forget to close the door when I enter the office.
			I often forget to close my hands when I enter the ATM pin.
			I often forget to close my bag when I open my bag.
		Work in a place that stores a lot of personal data	My work every day relates to company data (Example: HRD, Finance, IT).
	Coping and adaptation capacity (α = 0.632)	The ability to deal with people who threaten the security of personal data	I know how to protect myself when I am in danger.*
			I am able to guess if someone compromises my privacy security.*
		The ability to take follow-up	I will report to the authorities if I get an email or call from someone who asks for information that is not reasonable.*
Excitement of Victory (IV 1)	Affective (α = 0.702)	-	I easily receive an overflow of gifts.
			I will immediately follow the directions requested to get a prize.
Fear of authority (IV 2)	Affective (α = 0.716)	-	I will immediately follow the directions requested by legal officers without thinking.
			I trust people who have high authority so that if they ask for information I will immediately provide it.
Desire to be helpful (IV 3)	Affective (α = 0.624)	-	I will immediately help people who need help even though I don't know them.
			I will help my friend complete the information if my friend needs it in full.
Fear of loss (IV 4)	Affective (α = 0.653)	-	I am afraid of losing opportunities that I rarely get.

Variable	Dimension	Indicator	Item
			If I am only given 1 week to claim the prize that I won then I will not think long enough to follow the instructions requested.
Laziness (IV 5)	Behavioral (α = 0.691)	-	I easily get bored with repetitive activities but I must do them.
			If my friend asks for company information and I don't know much about that information I will let my friend search for him/herself through the access I have.
Insufficient knowledge/literacy (IV 6)	Cognitive (α = 0.629)	-	I am easily emotionally convinced by others.
			I feel it's okay to lose my logical/critical awareness as long as I get praise from others.
Ego (IV 7)	Personality (α = 0.576)	-	I did not participate in training on products owned by the company I work for.
			I do not understand the company system I work for.

Notes. *Unfavorable item (reversely scored/coded); DV = Dependent variable; IV = Independent/predicting variable

To measure **the independent/predicting variables**, i.e. **excitement of victory, fear of the authority, desire to be helpful, fear of loss, laziness, ego, and insufficient knowledge/literacy**, the Indonesian-language scales were derived from concepts mentioned in Table 1. The items are presented in the Table 2.

2.3. Data Analysis

Responses were denoted on a six-point Likert scale, ranging from "Strongly Disagree" (scored 1), "Disagree" (scored 2), "Somewhat Disagree" (scored 3), "Somewhat Agree" (scored 4), "Agree" (scored 5), to "Strongly Agree" (scored 6). Higher scores on dependent/criterion variables reflect higher psychological vulnerability, whereas higher scores on independent/predicting variables reflect increasingly higher vulnerability factors.

The researcher applied a predictive correlational study design using a self-report method. Data was analyzed through multiple linear regressions using *IBM SPSS Statistics 25 for Windows*.

3. Results and Discussion

Multiple linear regression analyses from this study's sample (noting that the generalization of this study's results might be limited to them and the ones with similar characteristics to this sample) showed that:

- There is a psychological model predicting the vulnerability of experiencing phishing (H1): $F(7, 261) = 8.332$, $p = 0.000$, $p < 0.01$, $R^2 = 18.7\%$. In the lifelong learning perspective, applications of this psychological model are common. Other models that simultaneously involve knowledge, motivation, and performance have been studied and are available in current literature (e.g. Bajis, Chaar, & Moles, 2020; Pouska, 2019; Ramírez Luelmo, El Mawas, & Heutte, 2020).
- There is a psychological model predicting the vulnerability of experiencing tailgating (H2): $F(7,261) = 8.513$, $p = 0.000$, $p < 0.01$, $R^2 = 19.0\%$.
- The excitement of victory (H3), desire to be helpful (H5), ego (H8), and insufficient knowledge/literacy (H9) cannot predict the vulnerability of experiencing phishing ($p > 0.05$; see Table 3).
- Fear of the authority (H4), fear of loss (H6), and laziness (H7) can predict the vulnerability of experiencing phishing ($p < 0.05$; see Table 3). Specifically, based on the values of the regression coefficient (β):
    - The higher the fear of authority, the higher the vulnerability to phishing.
    - The higher the fear of loss, the lower the vulnerability to phishing.
    - The higher the laziness, the higher the vulnerability to phishing.
- The excitement of victory (H10), fear of authority (H11), desire to be helpful (H12) cannot predict the vulnerability of experiencing tailgating ($p > 0.05$; see Table 4).
- Fear of loss (H13), laziness (H14), ego (H15), and insufficient knowledge/literacy (H16) can predict the vulnerability of experiencing tailgating ($p < 0.05$; see Table 4). Specifically, based on the values of the regression coefficient (β):
    - The higher the fear of loss, the lower the vulnerability to tailgating.
    - The higher the laziness, the higher the vulnerability to tailgating.
    - The higher the ego, the higher the vulnerability to tailgating.
    - The higher the insufficient knowledge/literacy, the higher the vulnerability to tailgating.
- Therefore H1, H2, H4, H6, H7, H8, H13, H14, H15, H16 were supported by empirical data.
- Therefore H3, H5, H9, 10, H11, H12 were not supported by empirical data.

Table 3. Multiple linear regression analysis predicting vulnerability to phishing (*n* = 262)

Predictor variable	***B***	***SE B***	***β***	***t***	***p***	***Tolerance***	***VIF***
Excitement of victory	0.295	0.274	0.083	1.075	0.283	0.534	1.874
Fear of authority	0.723	0.272	0.205	2.653	0.008	0.535	1.869
Desire to be helpful	0.276	0.287	0.069	0.963	0.336	0.630	1.586
Fear of loss	-0.752	0.316	-0.196	-2.381	0.018	0.472	2.119
Laziness	0.617	0.234	0.182	2.638	0.009	0.674	1.483
Insufficient knowledge/literacy	0.281	0.255	0.076	1.103	0.271	0.672	1.487
Ego	0.500	0.282	0.127	1.771	0.078	0.623	1.604

Note. VIF = variance inflation factor; *SE* = standard error

Table 3. Multiple linear regression analysis predicting vulnerability to tailgating (*n* = 262)

Predictor Variable	***B***	***SE B***	***β***	***t***	***p***	***Tolerance***	***VIF***
Excitement of victory	0.245	0.145	0.13	1.687	0.093	0.534	1.874
Fear of authority	0.126	0.144	0.067	0.872	0.384	0.535	1.869
Desire to be helpful	0.147	0.152	0.069	0.966	0.335	0.630	1.586
Fear of loss	-0.497	0.167	-0.244	-2.970	0.003	0.472	2.119
Laziness	0.285	0.124	0.158	2.295	0.023	0.674	1.483
Insufficient knowledge/literacy	0.283	0.135	0.144	2.090	0.038	0.672	1.487
Ego	0.413	0.15	0.197	2.757	0.006	0.623	1.604

Note. VIF = variance inflation factor; *SE* = standard error

3.1. The Statistically Significant Predictors

It was found that **the higher the fear of authority, the higher the vulnerability to phishing**. The fear of authority is a "habitual affective state" that grows in a person from an early age and consequently becomes a form of submission that arises when a power figure is present (Dayhoff, 2011; Kashtan, 2012). This predictor becomes significant when respondents feel intimidated by power, not just naming the "authority" alone (Shetty, 2011). It may also be influenced by a work factor, i.e. length of service ($M_{\text{length of work service}}$ = 2.29 year, $SD_{\text{length of work service}}$ = 0.763 years) that results in the emergence of loyalty and yield to authority. As increases in the predictor may influence a person's affective properties, which then increases vulnerability—therefore a person may follow any instruction given by an authoritative-like figure without any deliberation, and behave as loyal as they are expected to be (Naidoo, 2015).

It was found that **the higher the fear of loss, the lower the vulnerability to phishing**. In contrary to the researcher's assumption, the correlational direction is negative instead of positive. This may be due to external factors such as the entire sample's age group, whereby the range of 19-56 years (M_{age} = 28 years old, SD_{age} = 8.319) allows habituation (or familiarity) to phishing (Pattinson et al., 2012). Also, active social media exposure plays a role in lowering vulnerability to phishing (Ayaburi & Andoh-Baidoo, 2019; Russo, Binaschi, & De Angelis, 2019), considering that it is a source that regularly reports suspicious activities, and according to demographic data, participants use social media ranging from a minimum of 3 hours to a maximum of 24 hours; exceeding the ideal durational use of social media, which is approximately two hours (Limbong, 2018). Therefore, the higher fear of loss could cause an act of refusal to tempting offers such as winning prizes due to the intensity of social media exposure and similar past life experiences.

It was found that **the higher the laziness, the higher the vulnerability to phishing**. The individual tends to look for shortcuts to achieve something, or a tendency to easily feel bored and consequently seek to attain things effortlessly, as well as lack of confidence to achieve success from exerting effort through hard work, hence laziness functions to eliminate fear and feelings of helplessness (Burton, 2014; Shetty, 2011). When lazy individuals start to feel bored, they increase their vulnerability to an attacker as they exhibit a relaxed or non-threatening inclination. This individual might find a simpler way to achieve a position, such as prizes in form of money, dignity, making it easy for a schemer to attack people with these qualities—knowing that it will be easier to deceive the target and obtain the necessary information easily in exchange for gifts that are falsely promised or given (Gordon, 2018; Olaiya, Lamidi, & Bello, 2020).

It was found that **the higher the fear of loss, the lower the vulnerability to tailgating**. In contrary to the researcher's assumptions, the correlational direction is negative instead of positive. Loss of opportunities does not only revolve around materialistic objects but may encompass loss through death; relationship termination and divorce; job loss; life-threatening diseases and long-term disability; homelessness; lasting trauma and repetitive memories; retraction of rights and stigma planting; losses due to war and violence; and aging (Journal of Loss and Trauma, 2020; Meinecke, 2018). In this technological era, a large majority of the developed world has started using internet-based platforms to run some of their daily activities via the Internet. Various information about one's self from identity to financial data is registered in cyberspace (clouds), and the challenges of experiencing tailgating are already common. When someone loses their material possessions, it will harm and influence their psychological reality twice as much as when they feel lost compared to when they feel happy in winning something (van den Hoven, Blaauw, Pieters & Warnier, 2019). When a person loses his/her privacy, it is similar to that of losing money—harm is induced upon one's identity (Marvin, 2018). It is supported by the empirical data that 80% of total participants stated that they were indeed afraid of losing their privacy and consider that privacy is more important than material/price/reward loss (fear of loss) based on their responses to psycho-demographic questions. With this being said, when the respondents were exposed to a form of tailgating, they tend to protect their identity, safety, and personal data and this may lower vulnerability to tailgating (Aurigemma & Mattson, 2017; Kitteringham, 2008; Young, 2016).

It was found that **the higher the laziness, the higher the vulnerability to tailgating**. In the scale, there are items that translates to how respondents' do not feel suspicious towards their associates who access their rights as well as their private ownership (i.e. "*I will help my friend complete the information if my friend needs it in full*", or "*I trust people who have high authority so that if they ask*

for information I will immediately provide it") —in this case, it is the participants' computer—because they are too lazy to help their associates in providing information to them. The laziness to think long enough and feel disturbed by help requests from their associates and allowing others access their computers might lead to a situation where an attacker follows the employees—targets—who have legal access to a restricted area. Usually, attackers also offer "assistance" to reach a place that they cannot reach (Fahey, 2016). *Laziness* plays a role in these incidents, whereby it is easier for the attacker to carry out his actions when the target is lazy to do his job (Bisson, 2019).

It was found that **the higher the ego, the higher the vulnerability to tailgating**. This can be caused by the attacker's ability to create a schematic pattern that attacks the target's emotions and subsequently lower their capacity to think logically when the attack is being carried out (Shetty, 2011). The situational factors that causes a target to feel emotional, for example, feeling happy when being complimented, without thinking logically as to why the target is being complimented. Attackers who take advantage of this condition will easily probe or ask for help to access a location (Mailfence, 2016). The attacker can also bring or say something offensive to his/her "coworkers", and make the target not think long enough to respond to such manners (Bisson, 2019).

It was found that **the higher the insufficient knowledge/literacy, the higher the vulnerability to tailgating**. The target of tailgating usually is not well-informed about the critical information in their organization, making it easier for attackers to execute fraudulent schemes (Mailfence, 2016). This causes the attacker to manipulate the target by stating that the product or organization's system is set following the attacker's description of a product or system. Insufficient literacy can also be influenced by how little the target received information about social engineering and training to become more alert in facing attacks (Vielberth et al., 2019).

3.2. The Statistically Insignificant Predictors

It was found that the **excitement of victory cannot predict the vulnerability to phishing**. A sense of excitement that arises because of gifts that awaits can influence someone to experience a social engineering scheme (Shetty, 2011). When the excitement of getting a gift starts to increase, the vulnerability to phishing is also high. This is due to a distinctive element in phishing cases, where the attacker presents the gifts as attractive as possible and then demands the target to think quickly to attain the attractive prize. Hence, someone becomes vulnerable because they become impulsive with excitement. However, based on this study' analysis, it may be that for some people interpreting victory is a human nature that makes humans always want more than others when an ongoing competition is involved (TheGrandWazoo, 2011). However, no competition was implied in the scales' items. Also, the habituation (or familiarity) process (as mentioned before on the predictive-correlation between **fear of loss** and **vulnerability to phishing**) of one's experience can prevent the emergence of stimulation from feeling pleasure after winning a fraud scheme.

It was found that the **desire to be helpful cannot predict the vulnerability to phishing**. Some people who have altruistic motivations tend to prioritize others over themselves without expecting anything in return, and this results in the possibility of experiencing phishing (Bolino & Grant, 2016). They do not think long enough to help anyone without having prior knowledge of the person they help (Latané & Darley, 1970). However, when these altruistic people have the awareness of exposure to phishing from the information they receive from social media, this awareness might lead to an assessment of a potential target, raising doubts as to whether they should take any action (Bolino &

Grant 2016). Negative interpretations of the situation may cause someone prefer not to help (Latané & Darley, 1970).

It was found that **insufficient knowledge/literacy cannot predict the vulnerability to phishing**. Some people have less literacy about the products or systems from the organization they work for (Abass, 2018). When a target is asked for important information regarding the company they work for, but the target is not well-informed, the attacker will have difficulty to commit phishing—to obtain important information from the target. If some of the targets have received enough training or information exposure about the phenomenon (Moramarco, 2016)—by knowing what patterns cause a person to be deceived by a scheme or plan; situations like this make a lower the likeliness for them to experience phishing. By receiving training and information exposure about phishing on various platforms, potential targets or staff in general could become accustomed to avoid phishing.

It was found that the **(appeal to) ego cannot predict the vulnerability to phishing**. Some people who often respond receptively to compliments that play with emotions tend to put aside rational thinking and not think long enough about the reasons as to why they are being complemented. This causes a higher tendency to be more emotional, facilitating, or increases the likeliness of some people to experience phishing. However, phishing that is carried out via email or SMS may hinder the conveyance of emotional contact, so that the target's feeling of being more emotional is not elicited even when emails or SMSs have a sense of urgency, hence lowering vulnerability from the target's side (Lohani, 2019; Moramarco, 2016). The situation in the email environment may give "space" for one to not respond and prioritize logical or critical appraisal before becoming emotional and vulnerable (SecurityTrails, 2020). Furthermore, for others, the emotion as triggered does not necessarily cause people to abandon their logical thinking immediately, as the may even think skeptically towards the attacker. In Latané and Darley (1970), it was mentioned that negative interpretations may arise in the ideation of giving good things. From the explanation above, it can be assumed that the emotional feelings that arise are feelings of skepticism and suspicion (Halpern, 1993; Negrea-Busuioc, 2019; The Book of Life, n.d.). It can be concluded that emotional skepticism may lower the possibility to experience phishing.

It was found that the **excitement of victory cannot predict the vulnerability to tailgating**. This could happen due to the absence of stimuli relating to feeling victorious in the process of tailgating. In a situation where an attacker does not have proper authentication after following an employee to a restricted area and ask for help from them, tailgaiting attempts might fail due to the absence of competition (Sadiku, Musa, & Shadare, 2016). Tailgating is a social engineering technique that involves direct interaction where the attacker and the target must meet (SecurityTrails, 2020).

It was found that **fear of authority cannot predict the vulnerability to tailgating**. It might be because, in tailgating, the attacker usually acts as someone who does not have the authority ("superiority") or authentication to access a location in their work building, as they typically present themselves as the needy ("inferior") subject that requests or expects for help from the target in a typical fraud scheme (Bisson, 2019).

It was found that the **desire to be helpful cannot predict the vulnerability to tailgating**. In some cases, individual differences may account for this, as some people are inconsiderate, uncharitable, or self-serving, which contradicts the altruistic motive switch; and in a tailgating case, the attacker's scenario to raise a target's urgency to help others may fail (Bolino & Grant, 2016).

4. Conclusion, Recommendation, and Limitation

From this study's limited sample, it was concluded that vulnerability to phishing is predicted more by affective factors, namely fear of authority and fear of loss; while vulnerability to tailgating is predicted by more varied factors such as affective factors (fear of loss), behavioral (laziness), personality (appeal to ego), and cognitive (insufficient literacy). In the context of the learning environment, this finding implies that people need to know more about their personal affective attributes when online surfing and become aware of or pay attention to their psychological states when observing and acting in offline settings, as measures to lower the risk of phishing and being tailgated.

Regarding the lifelong learning gravity of preventing disruption through these social engineering schemes, this present study alarms us on the need for psycho-education, i.e. how to increase a good sense of security and how to anticipate disruptive acts from external parties (esp. potential attackers) in our every day life. Media literacy alone is inadequate for prevention efforts. For this reason, the authors suggest that there are affective and behavioral literacy aspects about one's self and others, with regard to raising awareness and enhance training among students and trainees in reducing the vulnerability to phishing and tailgating.

The lifelong learning perspective's objective relating to educational gravity on social engineering does not only revolve around an individual's ability to address social engineering. It also aims at enhancing psychological capital to master, utilize, and direct social engineering towards responsibility and towards trust on human kindness (Nickel, 2019). It does not work contrariwise; using one's knowledge and awareness as a rationale and driving force to act hazardously in the (cyber)security world (Velki & Romstein, 2019).

The contributions of this paper to the lifelong learning and social psychology literature are: (1) When social engineering is ubiquitous nowadays, this study's findings add perspectives that education and learning require literacy not only about the media and technology but also the people. This is very relevant in the Covid19 pandemic situation that heavily relies on online learning; (2) The study constructed reliable measurement instruments of psychological vulnerability to social engineering (phishing, tailgating) as well as media literacy and other predictors of the vulnerability, though additional validation procedures would aid in justifying the correspondence of concepts for sensitive quantitative data; (3) This present study provides a basis for collective training and learning in detecting and anticipating various phishing and tailgating challenges in the educational and work setting.

This study's findings are analyzed with a focus on numerous methodological limitations. First of all, the notably small sample size prevents the findings from being extrapolated and has a significant risk of voluntary response bias, as well as bias from the convenience sampling method. Risk of biases also includes the likeliness of the respondents to have access to Internet, predomination of one ethnic group (Javanese), and higher literacy due to educational background, therefore it lacks representativeness of groups who work in large corporations but have lower education levels, are minorities, and have less access to the Internet but have equal risks of receiving phishing and tailgating (e.g. cleaning service personnel, office assistants, etc.). These limitations can be managed by applying non-convenience sampling, and with more robust study designs with the use of standardized measurements, application of blinded randomized studies and with control groups to generate less biased findings on the relationship between psychological vulnerability to social engineering. As the

technological era critically needs technological crime intervention that is evidenced-based across all societal levels, it may start from building profiles for those at-risk of such crimes in a way that this study has attempted to do so.

Acknowledgements

This work was supported by Bina Nusantara University as a part of Bina Nusantara University's International Research Grant (in Indonesian: Penelitian Internasional BINUS/PIB) entitled "Corruption Prevention: The Roles of Media Literacy, Nostalgia, and Celebrity Worship" with contract number: No.026/VR.RTT/IV/2020 and contract date: 6 April 2020. This present study focuses on the Media Literacy. The ethical decree is stated in Article 1 Paragraph 3 of the Letter. The authors would like to thank Aqila Dhiya Ratu Hafishina-BINUSIAN 2023 for the initial translation of this article from Indonesian to English.

References

Abass, I. A. M. (2018). Social engineering threat and defense: A literature survey. *Journal of Information Security, 9*(4), 257-264. https://doi.org/10.4236/jis.2018.94018

Abomhara, M., & Køien, G. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4*(1), 65-88. https://doi.org/10.13052/jcsm2245-1439.414

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. https://doi.org/10.3390/fi11030073

Alfarizi, M. K. (2019, July 3). 6 Modus penipuan online, dari belanja sampai bajak WhatsApp. Retrieved from https://tekno.tempo.co/read/1220637/6-modus-penipuan-online-dari-belanja-sampai-bajak-whatsapp/full&view=ok

Alshorooqi, F., & Rawadieh, S. M. (2017). Media implications in Bahrain's textbooks in light of UNESCO's media literacy principles. *Journal of Social Studies Education Research, 8*(3), 259-281. Retrieved from https://jsser.org/index.php/jsser/article/view/232

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security, 66*, 218–234. https://doi.org/10.1016/j.cose.2017.02.006

Ayaburi, E., & Andoh-Baidoo, F. K. (2019). Understanding phishing susceptibility: An integrated model of cue-utilization and habits. *Proceedings of ICIS 2019: Cyber-security, Privacy and Ethics of Information SystemSS*, 15-18 December 2019, paper 3290. Retrieved from https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/43/

Bajis, D., Chaar, B., & Moles, R. (2020). Rethinking competence: A nexus of educational models in the context of lifelong learning. *Pharmacy, 8*(2), 81. https://doi.org/10.3390/pharmacy8020081

Bansla, N., Kunwar, S. & Gupta, K. (2019). Social engineering: A technique for managing human behavior. *Journal of Information Technology and Sciences, 5*(1), 18-22. https://doi.org/10.5281/zenodo.2580822

Basset, R. (2019, October 3). 5 common phishing techniques. Retrieved from https://www.vadesecure.com/en/5-common-phishing-techniques/

Bisson, D. (2019, November 5). 5 social engineering attacks to watch out for. *The State of Security*. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Bolino, M., & Grant, A. (2016). The bright side of being prosocial at work, and the dark side, too: A review and agenda for research on other-oriented motives, behavior, and impact in organizations. *The Academy of Management Annals, 10*(1), 599–670. https://doi.org/10.1080/19416520.2016.1153260

Burton, N. (2014, October 25). The psychology of laziness. *PsychologyToday*. Retrieved from https://www.psychologytoday.com/us/blog/hide-and-seek/201410/the-psychology-laziness

Dayhoff, S. (2011, March 28). Fear of authority figures in the workplace isn't just social anxiety. Retrieved from https://ezinearticles.com/?Fear-of-Authority-Figures-in-the-Workplace-Isnt-Just-Social-Anxiety&id=6123777

Edwards, C. (2019, April 4). Don't get caught: Beware the Facebook quiz scam that could get ALL your accounts hacked. *The Sun*. Retrieved from https://www.thesun.co.uk/tech/8790455/beware-facebook-quiz-scam/

Fahey, R. (2016). Phishing – technical details and motives. Retrieved from https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/technical-details-reasons-for-attack/#gref

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. https://doi.org/10.17705/1jais.00447

Gordon, J. W. (2018, August 15). How hackers are proving your laziness with SMS phishing. *Tektonika - HP*. Retrieved from https://www8.hp.com/uk/en/tektonika/index.php/2018/05/15/hackers-proving-laziness-sms-phishing/

Halim, D. (2019, March). Polisi ungkap kasus penipuan online terkait penjualan alat kesehatan yang tipu warga Meksiko. *Kompas.com*. Retrieved from https://nasional.kompas.com/read/2019/03/08/15384431/polisi-ungkap-kasus-penipuan-online-terkait-penjualan-alat-kesehatan-yang?page=all

Halpern, J. L. (1993). Beyond "detached concern": The cognitive and ethical function of emotions in medical practice. *Yale Medicine Thesis Digital Library*, 3360. Retrieved from http://elischolar.library.yale.edu/ymtdl/3360

Hammond, C. (2004). Impacts of lifelong learning upon emotional resilience, psychological and mental health: Fieldwork evidence. *Oxford Review of Education, 30*(4), 551–568. https://doi.org/10.1080/0305498042000303008

Hartik, A. (2020, June 5). Webinar yang dihadiri Wapres diduga diretas, UIN Malang minta penjelasan Zoom. *Kompas.com*. Retrieved from https://regional.kompas.com/read/2020/06/05/14442871/webinar-yang-dihadiri-wapres-diduga-diretas-uin-malang-minta-penjelasan-zoom

Heartfield, R., Loukas, G., & Gan, D. (2017). An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks. *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*. https://doi.org/10.1109/sera.2017.7965754

INFPC. (2020). Information security awareness. Retrieved from https://www.lifelong-learning.lu/Formation/information-security-awareness/en

Journal of Loss and Trauma. (2020). Aims and scope. *Taylor & Francis Online.* Retrieved from https://www.tandfonline.com/action/journalInformation?show=aimsScope&journalCode=upil20

Kashtan, M. (2012, August 16). Our habitual responses to authority. *PsychologyToday*. Retrieved from https://www.psychologytoday.com/us/blog/acquired-spontaneity/201208/our-habitual-responses-authority

Kavanagh, C. (2019). Stemming the exploitation of ICT threats and vulnerabilities: An overview of current trends, enabling dynamics and private sector responses. *United Nations Institute for Disarmament Research*. Retrieved from https://unidir.org/publication/stemming-exploitation-ict-threats-and-vulnerabilities

Kitteringham, G. (2008). Lost laptops = lost data: Measuring costs, managing threats. *Connecting Research in Security to Practice (CRISP) Report*, ASIS International Foundation, Inc., Alexandria, VA. Retrieved from https://www.asisonline.org/globalassets/foundation/documents/crisp-reports/crisp-lost-laptops-lost-data.pdf

Latané, B., & Darley, J. M. (1970). *The unresponsive bystander: Why doesn't he help?* New York: Appleton-Century-Crofts.

Limbong, S. T. (2018, December 7). Berapa lama waktu ideal menggunakan media sosial dalam sehari? Retrieved from https://www.klikdokter.com/info-sehat/read/3619374/berapa-lama-waktu-ideal-menggunakan-media-sosial-dalam-sehari

Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research, 4*(1), 385-393. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391

Lumen. (n.d). Early and middle adulthood. *LumenCandela: Boundless Psychology*. Retrieved from https://courses.lumenlearning.com/boundless-psychology/chapter/early-and-middle-adulthood/

Mailfence. (2016, October 18). Social engineering: What is tailgating? *Medium*. Retrieved from https://medium.com/@Mailfence/social-engineering-what-is-tailgating-7162c6047eee

Marhaenjati, B. (2019, November 26). Kerugian penipuan online mencapai Rp 36 miliar. *BeritaSatu*. Retrieved from https://www.beritasatu.com/yudo-dahono/megapolitan/587464/kerugian-penipuan-online-mencapai-rp-36-miliar

Marvin, G. (2018, August 15). Survey: People fear loss of personal data more than having their cars stolen. *MartechToday*. Retrieved from https://martechtoday.com/survey-people-fear-loss-of-personal-data-more-than-having-their-cars-stolen-222769

Meinecke, L. D. (2018, April 14). The uncanny fear of loss, part 1. *PsychologyToday.* Retrieved from https://www.psychologytoday.com/intl/blog/theory-and-praxis/201804/the-uncanny-fear-loss-part-1

Moramarco, S. (2016, April 27). Phishing definition and history. Retrieved from https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/

Naidoo, R. (2015, January). Analysing urgency and trust cues exploited in phishing scam designs. In Z. Zaaiman & L. Leenen (Eds.), *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 216-222). Reading, UK: Academic Conferences and Publishing Limited. Retrieved from https://www.researchgate.net/profile/Rennie_Naidoo/publication/281843032_Analysing_urgency_and_trust_cues_exploited_in_phishing_scam_designs/links/5bee4e67299bf1124fd5e85c/Analysing-urgency-and-trust-cues-exploited-in-phishing-scam-designs.pdf

Negrea-Busuioc, E. (2019). Review of #FAKENEWS. Noua cursã a înarmãrii [#FAKENEWS. The new arms race] by Alina Bârgaoanu. *Romanian Journal of Communication and Public Relations, 21*(2), 61. https://doi.org/10.21018/rjcpr.2019.2.277

Nickel, P. J. (2019). Trust in engineering. In D. P. Michelfelder & N. Doorn (Eds.), *Routledge companion to philosophy of engineering* (forthcoming). Routledge. Retrieved from http://www.academia.edu/38272832/Trust_in_Engineering

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo' Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences, 9*(2), 003. https://doi.org/10.35248/2155-6156.20.9.003

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18–28. https://doi.org/10.1108/09685221211219173

Pertiwi, W. K. (2019, October 30). Waspada, marak penipuan meminta kode OTP Gojek dan Grab. *Kompas.com.* Retrieved from https://tekno.kompas.com/read/2019/10/30/11315897/waspada-marak-penipuan-meminta-kode-otp-gojek-dan-grab?page=all

Pîrnau, M. (2017). Considerations on preventing social engineering over the Internet. *Memoirs of the Scientific Sections, 40*, 85-96. Retrieved from http://mss.academiaromana-is.ro/mem_sc_st_2017/8_Pirnau.pdf

Pouska, B. (2019). Book review: Transforming perspectives in lifelong learning and adult education: A dialogue by Formenti, L., & West, L. *Adult Learning, 30*(4), 183–184. https://doi.org/10.1177/1045159519861345

Proxsis Consulting Group. (2020). Waspadailah! Hantaman Serangan Cyber terhadap Indonesia. Retrieved from https://proxsisgroup.com/cyber-crime-indonesia/

Rachmatunnisa. (2018, February 15). Penipuan hadiah Go-Jek makan korban. Retrieved from https://inet.detik.com/cyberlife/d-3868865/penipuan-hadiah-go-jek-masih-makan-korban

Rafique, S., Humayun, M., Gul, Z., Abbas, A., & Javed, H. (2015). Systematic review of web application security vulnerabilities detection methods. *Journal of Computer and Communications, 3*(9), 28-40. https://doi.org/10.4236/jcc.2015.39004

Ramadhanny, F. (2020, May 28). UI tanggapi isu peretasan website fakultas. *DetikInet*. Retrieved from https://inet.detik.com/security/d-5032726/ui-tanggapi-isu-peretasan-website-fakultas

Ramírez Luelmo, S. I., El Mawas, N., & Heutte, J. (2020, July). Towards open learner models including the flow state. *Adjunct Publication of the 28th ACM Conference on User Modeling: Adaptation and Personalization UMAP '20* (pp. 305-310). https://doi.org/10.1145/3386392.3399295

Regmi, K. D. (2020). Social foundations of lifelong learning: A Habermasian perspective. *International Journal of Lifelong Education, 39*(2), 219–233. https://doi.org/10.1080/02601370.2020.1758813

Rigby, R. (2019, May 5). Psychology of wealth: Do the new rich not care about losing money? Retrieved from https://www.ft.com/content/9569eaaa-4009-11e9-9499-290979c9807a

Russo, L., Binaschi, F., & De Angelis, A. (2019). Cybersecurity exercises: Wargaming and red teaming. In A. Armando, M. Henauer, & A. Rigoni (Eds.), *Next gGeneration CERTs* (Vol. 54, pp. 44-59). IOS Press. https://doi.org/10.3233/NICSP190008

Safianu, O., Twum, F., & Hayfron-Acquah, J. B. (2016). Information system security threats and vulnerabilities: Evaluating the human factor in data protection. *International Journal of Computer Applications, 143*, 8-14. https://doi.org/10.5120/ijca2016910160

SecurityTrails (2020, August 20). Social engineering: What is it? Types of social engineering attacks and how to protect yourself from them. Retrieved from https://securitytrails.com/blog/social-engineering-attacks

Shetty, D. (2011). Social engineering. Retrieved from https://www.exploit-db.com/docs/english/18135-social-engineering---the-human-factor.pdf

Sinclair, V. G., & Wallston, K. A. (1999). The development and psychometric evaluation of the Brief Resilient Coping Scale. *Assessment, 11*(1), 94-101. https://doi.org/10.1177/1073191103258144

Sinclair, V. G., & Wallston, K. A. (2010). Psychological vulnerability predicts increases in depressive symptoms in individuals with rheumatoid arthritis. *Nursing Research, 59*(2), 140-146. https://doi.org/10.1097/NNR.0b013e3181d1a6f6

Smith, G. (2018). The intelligent solution: automation, the skills shortage and cyber-security. *Computer Fraud & Security, 2018*(8), 6–9. https://doi.org/10.1016/s1361-3723(18)30073-3

Tasevski, P. (2016). IT and cyber security awareness – Raising campaigns. *Information & Security: An International Journal, 34*, 7–22. https://doi.org/10.11610/isij.3401

Thapar, A. (2007). Social engineering: An attack vector most intricate to tackle! Retrieved from http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf

The Book of Life. (n.d.). Emotional skepticism. Retrieved from https://www.theschooloflife.com/thebookoflife/emotional-scepticism/

TheGrandWazoo. (2011, August 21), Psychology of victory. Retrieved from https://www.dailykos.com/stories/2011/8/20/1009042/-

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2019). Privacy and Information technology. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2019 Edition). Retrieved from https://plato.stanford.edu/archives/win2019/entries/it-privacy/

Velki, T., & Romstein, K. (2019). User risky behavior and security awareness through lifespan. *International Journal of Electrical and Computer Engineering Systems, 9*(2), 53–63. https://doi.org/10.32985/ijeces.9.2.2

Vielberth, M., Menges, F., & Pernul, G. (2019). Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity, 2*(23), 1-15. https://doi.org/10.1186/s42400-019-0040-0

Voskoboinicov, S., & Melnyk, S. (2018). Cyber security in the modern sociation and improvement of preparation of future factors in the field of competent approach. *Social Work and Education, 5*(1), 103–112. https://doi.org/10.25128/2520-6230.18.1.10

Winpenny, E. M., van Sluijs, E. M. F., White, M., Klepp, K-I., Wold, B. & Lien, N. (2018). Changes in diet through adolescence and early adulthood: Longitudinal trajectories and association with key life transitions. *International Journal of Behavioral Nutrrition and Physical Acticity, 15*, 86. https://doi.org/10.1186/s12966-018-0719-8

Wisner, B. (2016). Vulnerability as concept, model, metric, and tool. *Oxford Research Encyclopedia, Natural Hazard Science* (pp. 1-51). https://doi.org/10.1093/acrefore/9780199389407.013.25

Young, C. S. (2016). Information security threats and risk. In C. S. Young (Ed.), *Information security science: Measuring the vulnerability to data compromises* (pp. 3–27). MA: Syngress, Elsevier. https://doi.org/10.1016/b978-0-12-809643-7.00001-2