Personal and Ubiquitous Computing
https://doi.org/10.1007/s00779-024-01794-9

ORIGINAL PAPER

A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective

George A. Thomopoulos[1] · Dimitrios P. Lyras[2] · Christos A. Fidas[1]

Received: 13 March 2023 / Accepted: 27 February 2024

Abstract
Phishing is one of the most important security threats in modern information systems causing different levels of damages to end-users and service providers such as financial and reputational losses. State-of-the-art anti-phishing research is highly fragmented and monolithic and does not address the problem from a pervasive computing perspective. In this survey, we aim to contribute to the existing literature by providing a systematic review of existing experimental phishing research that employs EEG and eye-tracking methods within multi-modal and multi-sensory interaction environments. The main research objective of this review is to examine articles that contain results of at least one EEG-based and/or eye-tracking-based experimental setup within a phishing context. The database search with specific search criteria yielded 651 articles from which, after the identification and the screening process, 42 articles were examined as per the execution of experiments using EEG or eye-tracking technologies in the context of phishing, resulting to a total of 18 distinct papers that were included in the analysis. This survey is approaching the subject across the following pillars: a) the experimental design practices with an emphasis on the applied EEG and eye-tracking acquisition protocols, b) the artificial intelligence and signal preprocessing techniques that were applied in those experiments, and finally, c) the phishing attack types examined. We also provide a roadmap for future research in the field by suggesting ideas on how to combine state-of-the-art gaze-based mechanisms with EEG technologies for advancing phishing research. This leads to a discussion on the best practices for designing EEG and gaze-based frameworks.

Keywords Phishing · Eye-tracking · Electroencephalography · Human factors · Security and privacy

1 Introduction

Online deception attacks have attracted significant attention from researchers and extensive research has been conducted for more than twenty years. Nowadays, the rapid proliferation of email, web-based technologies, smart communication devices, and social media and the expanded utilization of artificial intelligence (AI) has assisted cybercriminals to generate more sophisticated deception methods and generate security threats that are increasingly difficult to detect. Published research suggests that such attacks, especially through AI technology tools, are far more professionally exploited compared to what becomes publicly disclosed [1, 2]. As the complexity of the cybersecurity domain rises, it is becoming more difficult to detect, analyze, and regulate fraudulent events [1]. While technological solutions can reduce the number of online deceptions, purely technical defense solutions can never be perfect.

Adequate defense against social engineering cyberattacks requires, among others, a deeper understanding of the interplay among human emotional and cognitive factors towards cyberattacks susceptibility. Simultaneously, efforts should be made to minimize or mitigate the resulting damage on both personal and enterprise levels [3]. Human decision-making serves as the final barrier against cyberthreats, prompting significant interest in investigating and comprehending whether and how human cognitive and emotional conditions generate neural processes that can be harnessed to reason about and potentially detect the underlying presence of a cyberattack [4]. As such, there is a particular research interest to leverage on brain computer interfaces and gaze-based

✉ George A. Thomopoulos
gthomop@upatras.gr

[1] Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

[2] Athens, Greece

Published online: 19 March 2024

apparatus, to early detect the possibility of a cyberattack and assist users for effective decision-making.

Based on recent analyses, phishing attacks are still the most widely and easy to perform cyberattacks, revealing the existence of over two (2) million phishing sites as of January 2021 [5], and it has become the scourge of the modern era, affecting a wide social spectrum of all classes and ages, in multiple methods and forms. Phishing is the practice of deceiving, pressuring, or manipulating people into sending sensitive information or assets to the wrong people by masquerading a message as legitimate. It refers to social engineering practices, by email, phone calls, or social media and text messages, pretending to be from trusted service providers, aiming to induce end-users to reveal personal information, such as passwords, pin codes, credit card numbers, and similar sensitive data. Phishing can be defined as a threat, which by virtue of social engineering techniques and/ or other technological or non-technological means, facilitates the attacker to retrieve personal information from her victims, causing them monetary or other damage because of this information leakage [6]. Albeit electronic phishing appeared almost two decades ago, similar techniques can be traced back at least to the nineteenth century. Exploring the history of pre-internet swindling schemes helps draw a bigger picture of the current phishing and scamming methods, with one of the most common nineteenth-century techniques being the "*Spanish Prisoner Letter*" [7]. Usually, phishing attacks are targeting a high number of "*victims*" and hence effective communication methods with extensive outreach are often preferred by the attackers. For example, they can be sent over e-mail, SMS (smishing), or leverage voice (vishing), and/ or social media channels (Facebook, Twitter, etc.) to deploy the attack. Typically, the intent is to steal the credentials or financial information from the users (aka identity thefts and cat-phishing). *Identity theft* involves stealing private information such as credit cards number, tax or social security numbers, name, address, date of birth, or other similar sensitive information aiming for the direct financial gain of the attacker, whereas *cat phishing* relies mainly on impersonating someone to ask victims to send money to the attacker [8].

Phishing has attracted significant attention from researchers and extensive work has been conducted with an exponential increase of phishing-related research papers during the last twenty (20) years (Fig. 1).

The topic of mitigating the effects of a phishing attack can be approached from several perspectives [9]. Numerous works on phishing mitigation tactics have been proposed that can be categorized under three main topics: i) *phishing filtering*, ii) *phishing detection support*, and iii) *user education and training*. *Phishing filtering approaches* leverage machine learning to detect and filter out malicious acts prior to being received by the end-users [10]. Examples include machine learning frameworks for scrutinizing webpages [11], phishing attack detection mechanisms based on natural language processing and machine learning [12], machine learning-based anti-phishing systems based on Uniform Resource Locator (URL) features [13], stacking models using URL and HTML features for phishing Webpage detection [14], and methods for detecting phishing certificates using certificate transparency logs [15].

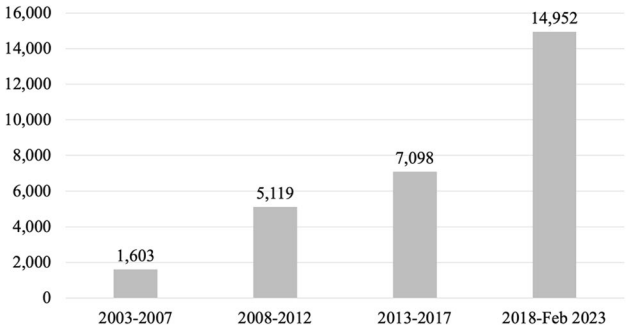

Fig. 1 Phishing research published during the last twenty (20) years indicating an exponential growth in number of scientific papers related to "phishing" research domain (results derived from ACM, Scopus, IEEE, Springer, Web of Science with search criteria: "phishing")

Phishing detection support tools typically assist users by providing them with information about a webpage or URL through Web browser warnings, intelligent agents, browser plugins, etc. Example works include the one of Althobaiti et al. [16] who investigated different approaches on how to more effectively express complex URLs and Web hosting concepts to users in a comprehensible way, the research of Yang et al. (2017) [17] who designed security warnings based on Website traffic ranks, the study of Althobaiti et al. (2018) [18] who proposed an intelligent agent that provides information about URLs with regards to the existence of misspellings, non-ASCII characters and redirection, and the research of Volkamer et al. (2017) [19] who proposed an extension for email clients that visually highlights the domain of a URL in an email and disables its hyperlink for three (3) seconds to make the users aware about the URL. Studies have also examined the effects of users' characteristics on susceptibility to phishing attacks, aiming to produce knowledge for designing personalized phishing detection support tools. Frequently studied user characteristics include user demographics such as gender and age, disabilities, technicalities, and digital inequalities. However, user demographics have not been proven to be decisive indicators on phishing susceptibility. Gender is often included as a demographic variable within phishing studies; however, results regarding its impact on phishing detection are again controversial, while some studies have concluded that a statistically significant relationship

between the gender and phishing susceptibility does exist [20–27], others have found no such connection [28–32].

Regarding the age differences, there results also controversial: Sheng et al. [24] at their study conclude that people between the ages of 18 and 25 are more susceptible to phishing than other age groups due to lower level of education, fewer years on the Internet, less exposure to training materials, and less of an aversion to risks. On the other end, Robinson et al. [25] implies that older adults exhibit disparities associated with access, usage, and skills so they are more likely to encounter challenges with technostress including managing passwords, maintaining online safety [25], and Lin et al. [14] at their study conclude that while young compared to older users showed greater susceptibility to scarcity (a belief that something is in short supply or almost gone), older compared to young users showed greater susceptibility to reciprocation (a need to fulfill repayment for a good or service received). Also, other factors may affect people's susceptibility to phishing like the differences in computer literacy based on which it has been shown that expert users tend to be more sensitive in detecting phishing emails [33], the users' cognitive abilities, according to which people with reflective reasoning may be in a better position to differentiate phishing emails compared to users with intuitive thinking [34] and the individual personality traits of the recipients of the attack, according to which users with higher conscientiousness are more likely to become phishing attack victims [21]. At the same time, studies indicate that the user disabilities, like people with autism are no parring or exceeding the average performance in the identification of the phishing websites [35] and blind people demonstrate robust reading strategies for identifying phish [36].

End-User education and training approaches as well as related frameworks have been proposed to support the decision-making of end-users towards more effective recognition of suspicious emails. Example works include dedicated training sessions during which the users are informed about the various existing phishing attacks and mitigation approaches [37]. Other training approaches aim to integrate learning and training aspects within the daily routines of the users (e.g., receive training in case the user is a victim of a phishing attack), rather than conducting a training beforehand [38]. Nevertheless, evidence suggests that educating and training end-users also entails several challenges and weaknesses. For example, studies have shown that individuals tend to forget the trained material and still fall for phishing attacks [39], while trainings that are integrated in daily routines are costly, given that administrations need to prepare and distribute simulated but at the same time realistic and up-to-date phishing attacks [14, 40].

1.1 Research motivation and contribution

Phishing research aims to design countermeasures against malicious attempts of trying to steal confidential information from people and to protect them from falling victims of it. Research shows that some users are more likely to disclose information than others when faced with an online scam and that personal characteristics are an important factor in mitigating the risk of phishing [9]. Considering the impact of phishing attacks on "human susceptibility," it is crucial to develop a comprehensive understanding of the process and characteristics of phishing itself, as well as the underlying human cognitive and emotional processes. Such scientific knowledge might facilitate the design of suitable and personalized anti-phishing security frameworks that consider the individual behavior of end-users, with a specific focus on emotional, cognitive, and personal factors. By leveraging on end-users' physiological responses reflected in brain- and/or gaze-based behavior during phishing tasks, it is possible to expedite the advancement of novel personalization methods and frameworks aiming to early differentiate between individuals engaged in malicious phishing activities and those who are not. This enables the implementation of effective countermeasures to enhance human decision-making capabilities.

In pursuit of this objective, our study delves into the potential efficacy of electroencephalography (EEG) devices in the context of phishing incidents. These devices enable the monitoring of neural activities and cognitive responses, thereby facilitating the inference of correlated brain reactions occurring concurrently during phishing encounters. Furthermore, we explore the utilization of eye-tracking technology, which captures spontaneous responses unaffected by conscious thought. This approach provides an alternative perspective for a comprehensive cognitive assessment of victims' reactions and stimuli in phishing scenarios. The integration of brain-computer interfaces and eye-tracking technologies has the potential to advance our understanding of cognitive processes and correlated brain responses beyond what either technology can offer independently. By combining these two modalities, we can benefit from improved temporal resolution and complementary information. The vision of this endeavor is to utilize real-time "brain-eye" measures, integrating brain and eye-tracking data, to develop a mechanism that evaluates the trustworthiness of a user's response while gaining insights into the role of neural measures and cortical activity in defending against phishing attacks. This holistic approach enables us to uncover the underlying mechanisms at work, advancing our understanding of how cognitive processes and physiological responses contribute to effective protection against phishing incidents.

Although several reviews have been identified in the research areas of phishing, electroencephalography (EEG),

and eye-tracking when examined individually [41–46], by the time of writing of this paper, we did not identify any systematic literature survey approaching the topic of phishing from both an EEG and eye-tracking perspective. Our intent in this paper is to identify experiments that were implemented in this area to investigate the correlation of EEG and eye-tracking against the most used phishing types. By analyzing the characteristics of these experiments, we aim to identify which brainiac and cognitive areas does phishing activate, expand our research to other types of phishing, correlate the brain's reaction to these phishing types, and make cognitive models which, through AI, can help improve on tactics for anti-phishing.

To this end, this study presents a survey spanning the last ten (10) years, with the aim of identifying phishing research papers that have considered in their study the experimental use of electroencephalography and/or gaze-based interaction, in order to set the stage for future anti-phishing frameworks that leverage collected EEG and gaze-based data to combat phishing. Our goal is to discover experiments conducted in the area of phishing types, determine which brain and cognitive areas phishing activates, extend our research to other types of phishing, correlate the brain's reaction to them, and create cognitive models that can help improve anti-phishing strategies by analyzing the characteristics of these experiments and mining their results.

The rest of the paper is organized as follows: in Section 2, we provide the theoretical background of our work, Section 3 gives a presentation of the electroencephalography and eye-tracking apparatus, Section 4 presents our research methodology and questions, Section 5 provides a systematic analysis of the existing phishing research related to our research motivation, Section 6 provides discussion and research suggestions, and in Section 7, we conclude with the main findings, further exploration of the applicability and generalizability of our findings and limitations of our work.

2 Theoretical background

2.1 Phishing classification

Phishing is a social engineering technique that through the use of various methods and techniques and aims at exploiting weaknesses of system processes with the aim to influence the end-users to reveal sensitive personal information (e.g., email address, username, password, or financial information) which subsequently can be used by the attacker to the detriment of the victim [47]. The logic of this terminology is that an attacker uses "bait" to lure the victim and then "ph-f-ishes" for their personal information [48].

Historically, the first instance of phishing was reported in 1995 when attackers attempted to convince victims to share their AOL account details [49]. The first use of the word phishing in printed media appeared in an article by Ed Stansel writing for the Florida Times Union and published on March 16th, 1997. The term phishing is derived from the word "fishing," spelt using what is commonly known as Haxor, which replaces Standard English characters with other ASCII characters: a typical rule in Haxor is that the letter "f" is converted to "ph." The origin of the word phishing is considered to be an extension to the word "phreaking" [50]. The use of "ph" in place of the "f" in the spelling of the term was used to link phishing scams with phreaks, which were some of the earliest hackers [51].

Phishing has a significant impact both in social and economic terms: Verizon's Data Breach Investigation Report for 2022 reports that 82% of the breaches involved the Social Engineering sector, with phishing contributing to more than 65% to it [52]. In the APWG (Anti Phishing Working Group) report for the 3rd quarter of 2022, a new record was reported (1,270,883 phishing attacks), which is the worst quarter ever reported [53]. In U.K. government's Cyber Security Breaches Survey published in 2022, 83% of businesses that reported some form of cyberattack in the preceding 12 months have also experienced a phishing attack as well [54]. According to the FBI, phishing emails are the most popular attack method used by hackers to deliver ransomware to individuals and organizations. Last, according to IBM's Cost of a Data Breach Report in 2021, phishing is fourth most common and second most expensive cause of data breaches, costing businesses an average of USD 4.65 million per breach.

2.1.1 Phishing classification

Several categorizations are registered with respect to the techniques employed for the phishing attacks. Abdillah et al. (2022) [45] in their research divided the phishing techniques into three groups (general, spear, and whale phishing) based on the attack target. *General phishing* is carried out with phishers massively trying to scam without using maximum effort or personalized means, indicating that the chances of success are meagre. This type of attack is most successful against typically less attentive users. *Spear phishing* targets a specific person (or a group of people) via a premeditated medium, often including information known to be of interest to the target, with the aim to intercept sensitive information. Due to the more personalized means of execution, this method has typically been perceived as more effective (compared to general phishing) in luring its victims. *Whale phishing* (whaling) targets high-level decision-makers within an organization that have access to highly valuable information and hence when successful it yields immediate, more valuable results for the attackers. A second categorization in the same study is based on the different means employed,

e.g., website, webpage, email, URL, SMS, and tweets. From a phishing attack survey that was conducted on the occurrences observed per type employed over the past 10 years, most of the occurrences were encountered in 2019 and 2020 by means of website (39%), webpage (22%), email (20%), URL (12%), and others (7%).

According to the researches from Alabdan (2020) [46] and Chiew et al. (2018) [55], phishing can be broken down into three main components. The first component is the *medium*, meaning the method (e.g., voice, SMS/MMS, and Internet) by which the phisher interacts with the target. The second component is the *vector*, that is the channel through which the phishing attack is conducted, with the main categories being vishing, smishing, email, instant messaging, social networks, and websites. *Vishing* is the method of phishing that uses the voice, either through a traditional phone device, mobile, or a VoIP. VoIP is a low-cost solution that can effectively obscure the actual physical location of the caller and can be almost indistinguishable compared to legitimate calls. *Smishing* is the use of SMS/MMS for the phishing attacks and can be implemented by sending a message to a victim (pretending to be originating from a trusted authority) or by sending a message that contains malware (or similarly that contains links to a website infested with malware). *Instant messaging (IM)*, compared to the vectors mentioned above, enable attackers to leverage audio, video, emojis, photos, files, and hyperlinks in their phishing attacks, which in turn may yield higher effectiveness into captivating the victim's attention and hence more effectively allure them to reveal personal information. *Social networks* allow people to communicate, connect, and share experiences and are hence an exceptional resource for phishers to identify group of targets and approach victims. Finally, fraudulent *Websites* are also often preferred by attackers, masked in such a way that renders them to appear as legitimate and which can then be used to intercept personal details when user-victim attempts to login or visit them.

The third component according to Alabdan (2020) [46] and Chiew et al. (2018) [55] is the *technical approach* that the phishers employ to gain access to the victim's personal details, with the main categories being spear phishing, whaling, business email compromise (BEC), QRishing, social engineering, man-in-the-middle, and mobile phones. The technical approaches may function independently or as a combination of them. *Business email compromise (BEC)* is a sub-type of spear phishing that focuses on governmental services, commercial organizations, or other big entities, aiming to compromise the corporate emails of their employees and use these in the attackers' favor. *QRishing* is a phishing attack relying on the fact that QR codes are challenging to be interpreted before being deciphered by a QR code reader, and on the fact that many QR readers are not seeking for the user's approval before accessing the QR code's content, thus leading the victim to malicious URLs engineered by the attacker. *Social engineering* is one of the oldest techniques available to phishers and is defined as the manipulation of a person by abusing the victim's emotions, gullibility, charity, or trust. In the *man-in-the-middle* attack, a malicious user intercepts a direct communication between two parties, meaning an end user (victim) and a service provider. The attacker then reconfigures the data used by the victim and contacts the service provider pretending to be the legitimate user of the service, with the intent to steal their credentials, account information, financial data, and/or use the resources authorized by the service to the legitimate user. The most common form is call phishing, where phishers pretend to be a legitimate organization such as a bank or tax agency and instruct the user to share their personal and sensitive information.

On another research, Aleroud et. al. (2017) [47] propose a phishing taxonomy where an attack can span across four dimensions: communication media, target environments, attack techniques, and countermeasures. In *communication media*, seven types are identified from the literature, meaning E-mails, websites, instant messaging (IM), online social networks, blogs and forums, mobile, and voice over IP. Among them, emails and websites are the means the most frequently studied. The *target environment* relates to the physical device(s) which the victims use to interact with and can be classified as: personal computers (PC), smart devices, and typical voice devices (e.g., desk phones). *Attack techniques* are grouped into three categories based on their purpose, meaning attack initialization, data collection, and system penetration. For *attack initialization*, the most commonly employed techniques include the usage of spoofed URLs, bogus IVR, social networking, man in the middle attack (MITM), spear phishing, spoofing mobile browsers, and embedded web contents. *Data collection* techniques aim to gather sensitive data from the victim and mainly rely on creating fake web forms, key loggers, recorded messages, automated social engineering bots, and fake event invitations. Finally, *system penetration* techniques are used in order to exploit system resources that can later be leveraged to further facilitate subsequent phishing attacks and fall in two main categories: *Fast-Flux*, which is DNS related technique that protects phishing sites from taking down by hiding the hosting machine of phishing websites and *cross-site scripting* in which malicious scripts are injected into otherwise benign and trusted websites, usually when an attacker uses a web application to send malicious code.

In Fig. 2, we present a detailed analysis of the variations of phishing attacks, based on the three examined taxonomies, showing all the interlinks between the vectors (channels) through which the phishing attack is conducted, the mediums exploited during a phishing attack and the technical approaches that the phishers employ to gain access to

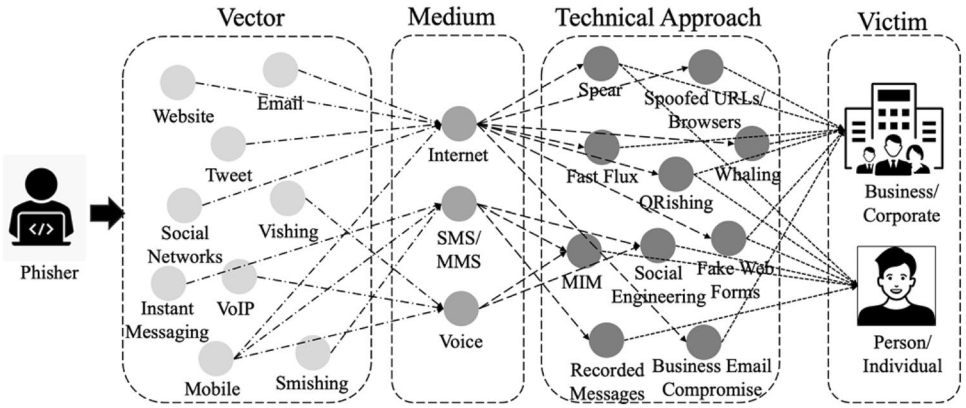

Fig. 2 Detailed analysis of the variations of phishing attacks showing all the interlinks between the vectors through which the phishing attack is conducted, the mediums exploited during a phishing attack and the technical approaches that the phishers employ to gain access to the victim's personal details

the victim's personal details. As shown in the figure, in the context of a phishing attack, a victim can be a target of a combination of technical approaches (from one or multiple vectors) that may be used by the phisher aiming for a better success rate. The knowledge of these interlinks is important to develop countermeasures that target each specific vector and to introduce policies and guidelines that prevent system or infrastructure exploitations from malicious activities.

3 Electroencephalography and eye-tracking apparatus

3.1 Electroencephalography apparatus

Albeit the first human EEG was recorded by Hans Berger in 1924 [56], electroencephalogram as a concept emerged in 1875 when Richard Caton reported in the British Medical Journal that animals with exposed cerebral hemispheres present electrical phenomena. EEG employs the principle of differential amplification or recording of voltage differences between distinct cerebral points operating a pair of electrodes that compares one active exploring electrode site with another neighboring or distant reference electrode. EEG belongs to the technology of brain-computer interfaces (BCI), which provides the brain with a non-muscular communication channel for conveying messages and commands to the external world. It is a non-invasive BCI method where a typical signal is used as an input for BCI applications and refers to the electrical activity recorded through electrodes positioned on the scalp, for measuring postsynaptic brain activity from the surface of the scalp associated with task-related or internal stimulation. This technique is used to measure different types of neural activities such as evoked responses (ERs), also known as evoked potentials (EPs) [57]. The EEG's temporal resolution is higher than many other brain imaging methods because it is simple, non-invasive, portable, and cost-effective. Also, EEG method takes milliseconds to depict changes in contrary to other methods that may experience a delay on the order of seconds or minutes, and because of this, it is often used to evaluate the time course changes in brain activation across different brain regions.

Typical EEG arrangement includes a cap carrying contact electrodes and wires, which are used to connect the contact electrodes to amplifiers that improve the quality of acquired signals and convert the signals through an analog-to-digital transformation, that allows brain signals to be stored on a computer for further research [57]. The types of electrodes that are used to acquire the brain signals are wet electrodes that are attached to the scalp with conductive pastes and often special caps, or dry electrodes that do not require any conductive gel. The dry electrode technology achieves excellent standards comparing to wet electrodes and reduces the time to apply sensors and enhances user comfort [58]. The electrodes can be arranged on the scalp following one of the international 10–20, extended 10–20, international 10–10, and international 10–5 standards. In these standards, the locations on a head surface are described by relative distances between cranial landmarks.

The international 10–20 system (Fig. 3) was the first standardized system that was first presented at the 2nd International Congress of IFSECN in Paris in 1949 and published by Jasper in 1958 [59]. The system is based on the relationship between the location of an electrode and the underlying area of cerebral cortex. The numbers "10" and "20" refer to the fact that the distances between adjacent electrodes are either 10% or 20% of the front-back or right-left distance of the skull. The primary purpose of the 10/20 system is to provide a reproducible method for placing a relatively small number (typically 21) of EEG electrodes. In 1991, an extension to the original 10–20 system was accepted by the American Clinical Neurophysiology Society (ACNS) and by the International Federation of Clinical Neurophysiology (IFCN) which involved an increase of the number of electrodes from 21 up to 81. This extended the "10–20" system of electrode placement by what is known as the "10% system" and referred as "10–10" system. However, high-end

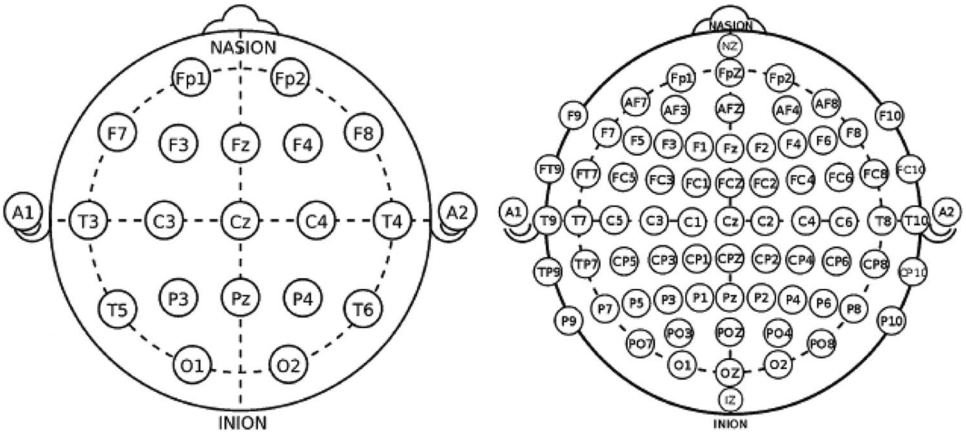

Fig. 3 The international 10–20 EEG placement system. Left panel: the 10–20 system or international 10–20 system. Right panel: modified combinatorial nomenclature system (MCN) 10–10 system. Each electrode placement site uses 1, 3, 5, 7, and 9 for the left hemisphere and 2, 4, 6, 8, and 10 for the right hemisphere and has a letter to represent the specific lobe or area of the brain: frontal (F), temporal (T), parietal (P), occipital (O), and central (C). Suffixal (Z) sites referring electrodes placed on the midline sagittal plane of the skull (Fz, Cz, Pz, and Oz) are present mostly for reference/measurement points [54, p. 75–76]

users still needed even higher density electrode settings, and hence in 2001 an extension to the "10–10" system was proposed, namely, the "10–5" system, enabling the use of more than 320 electrode locations [60].

The changes in EEG signals are highly associated with different cognitive functions, such as perception, emotion and cognition [61]. Table 1 lists the EEG wave properties analyzed by frequency band (measured in Hz), the corresponding brainiac region, and the states that relate to different human activities [61, 62].

3.2 Eye-tracking apparatus

Eye-tracking is an experimental method of observing and recording the eye motion and the allocation of visual attention. An eye-tracker measures where, how, and in what order gaze is being directed during a specific task, rendering the eye-tracking apparatus a reliable tool for investigating problems related to the visual attention, behavior, needs, emotional states, desires, and cognitive processes of a person. Cognitive processes such as perception, memory, language, and decision-making are known to be influenced by gaze behavior [63]. Eyes reflect mental processing of whatever is looked at any given moment and this makes eye-tracking broadly applicable to most researches that explore mental processes. Because of its high temporal sensitivity, eye-tracking not only reveals indications of the outcome but also provides a moment-by-moment insight into the unfolding cognition [64].

In the past twenty (20) years, the use of eye-tracking in various fields of research has received increased interest by the research community. Improvements in the eye-tracking technology have made it more affordable and user-friendly for participants and researchers. Recent technological advancements in hardware and software have contributed to the development of eye-tracking applications. Cumbersome, slow, and expensive equipment have been replaced by inexpensive, unobtrusive, and wearable devices, which produce meaningful data for subsequent analysis [65].

Table 1 EEG wave properties analyzed by frequency band (measured in Hz), the corresponding brainiac region and the states that relate to different human activities

Brain wave band	Frequency (Hz)	Brainiac region	Users' cognitive state
Delta	0–4	Front region	Dreamless sleep, non (rapid eye movement) REM sleep, unconsciousness
Theta	4–8	Free of task regions	Idling, actively trying to repress, response reaction, dreaming, imagining
Alpha	8–13	Both hemispheres, posterior regions	Relaxation, resting eyes closed
Mu	8–13	Sensorimotor Cortex	Alert, anxiety, concentration, working, idle hands and arms
Beta	13–30	Both hemispheres frontal lobe	Thinking
Gamma	30–100	Somatosensory cortex	Two senses combined, object recognition, short memory matching

Additionally, recent advances in computing capabilities enable the integration of machine learning algorithms (ML) into eye-tracking devices, rendering them into intelligent eye-tracking devices, and various hardware and software approaches have been implemented by research groups and companies [66]. Nowadays, the most popular eye-tracking system is the head-mounted video-based tracker that may be used in daily activities. Four eye-tracking techniques have been the focus of most studies in this field and in developing novel eye-tracking applications. These are the scleral search coil (SSC), infrared oculography (IOG), electrooculography (EOG), and video-oculography (VOG) [66]. Table 2 summarizes these techniques, how they work, advantages and disadvantages of each, and applications that they are typically used for.

The most prevailing gaze-based metrics that are utilized in the literature [65, 67] are presented in Table 3.

4 Methodology and research questions

This survey performs a systematic analysis of existing works that embraced unimodal (EEG or eye-tracking) or multimodal (combination of EEG and eye-tracking) apparatus for phishing research, thus approaching the subject across the three pillars as shown in Fig. 4. The first pillar refers to the experimental design practices with an emphasis on the applied EEG and eye-tracking acquisition protocols. More analytically, it examines the EEG device and montage as per the electrode placement and the number of channels, the type of eye-tracker most often employed (portable, desk-mounted), and eye-tracking method used and examines the users background such as number of participants in the experiments, the users' demographic data contrasted against the primary task of users, and the research question attempted to be answered from within the experiment.

The second pillar refers to the artificial intelligence and signal preprocessing techniques applied in those experiments. According to this pillar, the survey studies the analyzed channels of the examined EEG system, the existence of reference and ground electrodes, the participants' eye-tracking metrics as a response to the exposed phishing attack type, which preprocessing methods were employed, which feature extraction and classification methods were most applied in the considered experiments, and the accuracy that was reported per experimental setup.

The third pillar refers to the phishing attack types. From this perspective, we try to identify the phishing attack types and the relation these can have on the activation of specific brain areas and examine the participants' eye-tracking metrics as a response to the exposed phishing attack type.

Table 2 Eye-tracking techniques used in developing eye-tracking applications, how they work, advantages, disadvantages and applications typically used for

Technique	Method	Advantages	Disadvantages	Applications
Scleral search coil method (SSC)	Measures the magnetic field from small coils of wire embedded in a modified contact lens or anulus	High accuracy, good resolution, 3D data representation, high sampling rate	Complicated implementation, invasive, need for expensive gear	Healthcare and medical, research
Infrared oculography (IROG)	Measures the strength of an infrared light that is mirrored from the sclera	Handle eye blinking, used in light and darkness	Unable to quantify torsion movement, invasive	Healthcare and medical, HCI, and accessibility
Electrooculography (EOG)	Sensors attached to the area that surrounds the eyes detect an electric field while the eyes are rotating	Practicable, inexpensive, easy to use	Not for daily use, eye drifts limited, eye conditions limited, invasive	Healthcare and medical, HCI, and accessibility
Video-occulography (VOG)	Estimation of the direction of gaze from pictures delivered by a video camera	High accuracy, observing eye movement disorders, easy to use, allows head movements, fully remote recording, invasiveness	Expensive, high computational capabilities, eye torsion cannot be measured with closed eyes	Education, car assistant, HCI, and accessibility

Table 3 Potential eye-tracking metrics and indicators to measure cognitive load

Metric	Determination	Indicators
Gaze point	The number of rows captured by the ET device	One gaze point is one row captured by the ET
Fixation	A period in which eyes are fixed at a particular object in a stimulus	Typically, fixation duration is 100 to 300 ms
Smooth pursuit	An eye movement that allows eyes to closely follow a moving object	
Saccades	The rapid eye movements between fixations	Can be used to study reading behavior as early or expert readers
Scan paths	The sequence of fixation saccade-fixation	
Heat maps	The static or dynamic or static aggregations of gaze points and fixations that generates the distribution of visual attention	Shows maximum attention area of the stimulus
Area of interest (AOI)	Subregions of a stimulus object displayed on screen defined by user	Evaluated with the performance of two or more specific areas in the same picture, website or any program interface
Fixation sequence	A sequence generated based on fixation position and time information	Reflects salient elements in the display or in an environment that catch much attention
Respondent count	The number of respondents that has gaze direction towards a specific AOI	Higher respondent count indicate that fixations and gaze points are driven by some external aspects in the stimulus
Time spent	The amount of time that respondents spend on a specific AOI	Indicates motivation and conscious attention because long prevalence at a region points to a high-level interest

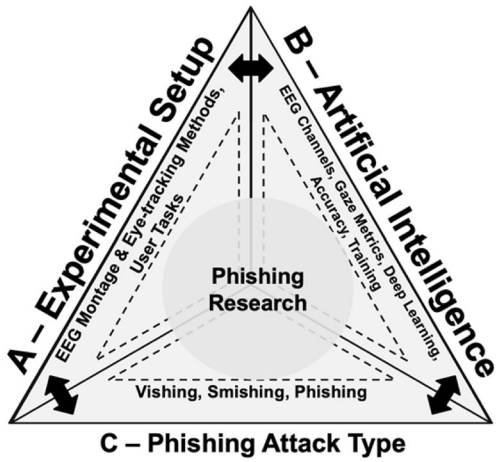

Fig. 4 The research model that was elaborated for a systematic analysis of existing works that embraced unimodal (EEG or eye-tracking) or multimodal (combination of EEG and eye-tracking) apparatus for phishing

4.1 Research questions

Based on the aforementioned research model, we formulated the following research questions related to the application of EEG and/or eye-tracking technologies against Phishing attacks:

RQ1: Which are the most applied experimental setups and how are these related with a) the number of participants, b) the EEG montage and/or eye-tracking setup, c) the EEG metrics and eye-tracking metrics employed, and d) the performance of these experiments. *By answering this research question, we will be able to provide insights on the most effective means for coping with each of the most employed phishing schemes as well formulate a solid spring broad for new researchers entering the field to obtain a better overview of the current state-of-the-art on the subject.*

RQ2: What are the investigated phishing attack types and how do they relate to cognitive processes and brain activity? *By answering this question, we can identify what type of phishing is dominant in the interests of the research community and the white space in phishing types of research in terms of the cognitive and brain responses.*

4.2 Research methodology

4.2.1 PRISMA setup process

Several well-known digital library databases were selected for the literature search, and the selection was based on their relevance to the computer science community. We performed a systematic search within the following digital libraries: Elsevier ScienceDirect, IEEE Xplore, ResearchGate, Springer, and the ACM Digital Library. To ensure compliance with research standards, PRISMA method [68] was employed. As the main research objective of this review is to examine articles that contain results of at least one EEG-based and eye-tracking-based experimental setup within a phishing context, the following keywords were selected: [*phishing AND EEG], [phishing AND "eye-tracking" OR eye-tracking], [phishing AND BCI].*

The initial process for our data collection began as a broad search for the term n1 = [phishing AND "eye-tracking" OR "eye-tracking"], n2 = [phishing AND EEG], and n3 = [phishing AND BCI] in Elsevier ScienceDirect, IEEE Xplore, ResearchGate, Springer, and the ACM Digital Library Databases. This generated 651 articles. From the initial search, we excluded duplicate records, articles that were not from journals or conference papers (e.g., books and presentations) and these that were from a different domain (e.g., health, social sciences, psychology, and education) coming up with a total of 327 papers.

4.2.2 PRISMA screening process

From this collection, we performed via manual supervision rather than the employment of any automated means, title, abstract, and full-text screening to identify papers that satisfied our inclusion and exclusion criteria. To be included, a paper needed to be primarily focused on the topic of phishing. The following inclusion criteria were used to identify and extract the useful literature from the search string: research articles should be in conference or journal, they should investigate phishing as well include references to EEG, eye-tracking, eye gaze, and BCI aspects and should have been published in the last ten years (2012–2022). Papers were excluded if the above inclusion criteria were not fulfilled and if they were an extended abstract or a work in progress, the primary language in which they were written was not English or they were found not to be related to phishing, even if they mentioned phishing somewhere in the paper. After applying the inclusion and exclusion criteria on the collected sample of 327 papers, 285 papers were excluded, and 42 papers were finally selected to be further processed. From a full-text eligibility on these papers, 29 papers were excluded for not containing any experiments; thus, 13 experimental papers remained for the course of the study. From the full-text study of the papers, 5 papers were added that were found in the references of the examined papers, so the number of papers that included in our SLR was 18 (Fig. 5).

Based on the PRISMA selection method outlined above, five (5) research papers have been retrieved that utilize experimental designs embracing an EEG apparatus in phishing research. Moreover, thirteen (13) research papers employ eye-tracking devices in their experimental setup. From the total of eighteen papers, two (2) rely on both methodologies, resulting to 16 papers studied (please see Table 4).

5 Analysis of results

5.1 RQ1: EEG and eye-tracking experimental design practices in phishing

5.1.1 Phishing and EEG

To obtain data with satisfactory quality, it is important to choose the right representative samples under the spectrum of demographic characteristics and other factors. All five (5) experiments examined in our survey followed the standard procedure of recording the demographic data of

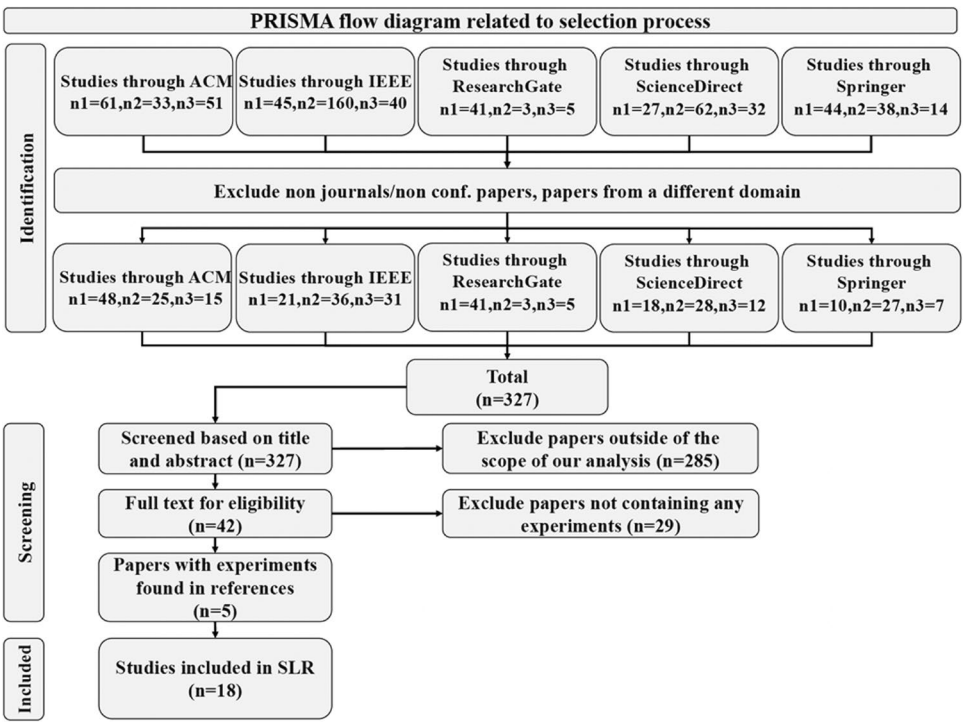

Fig. 5 PRISMA flow diagram related to selection process, where n1, n2, n3 denotes search criteria: n1 = [phishing AND "Eye-tracking" OR eye-tracking], n2 = [phishing AND EEG], and n3 = [phishing AND BCI]

Table 4 The 16 research papers studied and relevant utilized apparatus (x stands for the approach examined in each study)

Research paper	Utilizing EEG	Utilizing eye-tracking
Neupane et al. (2015) [69]	x	x
Rahman et al. (2018) [70]	x	
Valecha et al. (2020) [71]	x	
Sun & Yeh, (2017) [72]	x	
Hashem et al. (2017) [73]	x	x
Ramkumar et al. (2020) [74]		x
Alsharnouby et al. (2015) [75]		x
Miyamoto et al. (2014) [76]		x
Darwish & Bataineh (2012) [77]		x
Pfeffel et al. (2019) [78]		x
Miyamoto et al. (2015) [79]		x
McAlaney & Hills (2020) [80]		x
Huang et al. (2022) [81]		x
Yang et al. (2022) [17]		x
Anderson et al. (2013) [82]		x
Xiong et al. (2017) [83]		x

the participants. Most of the literature reviewed exhibited a higher proportion of male participants, outlining a gender imbalance. However, due to conflicting research findings regarding the influence of gender on phishing detection, it would be intriguing to validate the experimental results using a more representative sample that encompasses a broader range of genders. Similarly, the *age* varied between 18 and 34 years in all papers included in our analysis; nonetheless, an interesting conclusion was highlighted in [69], where the researchers observed differences in the participants belonging to each of the 19–22 and 30 + age groups, which may indicate that future studies might be needed to support these findings, especially considering the fact that as stated to our introduction, there are controversial results regarding the age differences. Regarding the participants' *background*, they were mainly university students, which albeit justifies the lower age groups examined, at the same time opens the question for further experimentation against other age groups, aiming to assess the generalizability of the study and to address questions on the effectiveness of these methods to a wider (age wisely) population.

5.1.2 EEG-montage and preprocessing

With respect to the EEG montage, it is important to analyze the electrode placement and the number of channels, because they can provide details about which brain areas are activated during a task and what is the relationship between the brain activities and the specific task. As shown in Table 5, most experiments use the "10–20" international system's [59] brain electrode distribution, whereas the number of electrodes used ranges from 2 to 256 and the sampling rate varies from 256 to 1000 Hz. Neupane et al. (2015) [69] uses EEG headset that is utilizing 10 channels of data, meaning Fz, F3, F4, C3, Cz, C4, P3, POz, and P4 sites to collect EEG data with a 256-Hz sampling frequency, Rahman et al. (2019) [70] utilizes 14 channels of data, meaning AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4 with two sensors as reference, with mostly the frontal lobe and parietal lobe sensors (AF3, F3, FC5, F7, P7, and P8) highly activated for the phishing detection task, Valecha et al. (2020) [71] uses an EEG headset with a 64-electrode cap, with a 500-Hz sampling frequency and Sun and Yeh (2017) [72] utilize 2 electrodes with sampling 512-Hz frequency. Finally, Hashem et al. (2017) [73] use EEG headset that follows the 10–20 (Geodesic) EEG system with 256 electrodes and a 1000-Hz sampling frequency. Regarding the reference electrodes, although several studies [84] indicate that the selection of reference electrode(s) can affect the estimation of certain EEG measures (e.g., connectivity), reference electrodes have not been recorded in most of the experiments performed, with the exception of the study of Rahman et al. (2019) [70].

EEG recordings tend to contain noise and artifacts which may often affect the experimental analysis and results. Therefore, it is essential to apply preprocessing and denoising to eliminate such artifacts as well as any additional noise

Table 5 Design of experiments and accuracy achieved in phishing and EEG experiments, asterisk denotes classification method that yield the highest accuracy from within the methods evaluated in each study. Columns: I. EEG-placement, II. no of exploited channels, III. Sampling (Hz) IV. Preprocessing, V. Feature extraction, VI. Classification, and VII. Accuracy

	I	II	III	IV	V	VI	VII
[69]	10–20	10	256	S/W	S/W	S/W-QDA	69%
[70]	10–20	14	N/A	AAR, butterworth	Tensor decomposition	BayesNet, logistic regression, Rip, IB1, random forest*	97%
[71]	10–20	64	500	ICA	ICA	ICA	N/A
[72]	10–20	2	512	S/W	S/W	S/W	N/A
[73]	10–20	256	1000	Low- & high-pass filters	WPD	SVM*, k-NN, random forest, bagging predictors	99%

from the electromyography (EMG) and electrooculogram (EOG) samples. Aiming to address RQ_1, in the context of the present survey, we investigated which preprocessing methods were employed in the literature examined in our survey. As shown in Table 5, MATLAB toolboxes, low-pass or high-pass filters and a variety of similar proprietary software tools (e.g., B-Alert Lab (BAL) Software provided by ABM, ThinkGear technology) tailored to the preprocessing task were used for this purpose.

5.2 Feature extraction, classification, and accuracy

Similarly to preprocessing, in emotion recognition analyses that rely on EEG signals, feature extraction is often considered beneficial towards improved emotion classification performance [85]. For our research and aiming to address RQ_1, we investigated which feature extraction and classification methods are most applied in the considered experiments as well as noted the accuracy that was reported per experimental setup. As shown in Table 5, WPD with MATLAB [73], PARAFAC 2 [70], and ICA [71] are used for the feature extraction task and several methods (including Bayesian regression, lazy/ensemble learning, and others) are used for classification. Hashem et al. (2017) [73] examines four different classification algorithms (support vector machine (SVM), *k*-nearest-neighbors (k-NN), random forests, and bagging predictors), with SVM succeeding the highest accuracy (99.77%). Rahman et al. (2019) [70] compared five classifiers, (BayesNet, logistic regression, JRip, IB1, and random forest) with the best performance being yielded by the random forest classifier (97% in terms of classification accuracy). Finally, Neupane et al. (2015) [69] use quadratic discriminant function classification algorithm (QDA) for their analysis, reporting a classification accuracy of 69.69%.

5.2.1 Phishing and eye-tracking

Based on the PRISMA selection method outlined at Section 4.2, thirteen (13) experiments have been identified relevant to eye-tracking apparatus, containing evaluation for the reviewed phishing attack types.

Participants demographics The number of participants in these studies ranged between 20 and 30, where the age range was between 18 and 34 years, reporting a mean age of ~ 20 years old, which is representative of the group of users who use Internet frequently and who are supposedly more vulnerable to phishing attacks. Alsharnouby et al. (2015) [75] find no statistical significance between participants' ages and their scores whereas Neupane et al. (2015) [69] identifies differences between the participants belonging to the 19–22 age group and those aged more than 30, which indicates some white space for further experimentation as per the effect the age could have on such phishing attacks. Our analysis of the reviewed papers revealed an imbalance in the representation of genders, with a predominant focus on male participants in eight experiments, while in one experiment [80] 90% of their participants were female, and in four experiments [17, 73, 81, 82], the gender was not recorded. Finally, Huang et al. (2022) [81] in his experiment is diversifying the participants (concerning their race, gender, and age) and adopts the feedback loop of Bayesian optimization to make a more comprehensive study of the human behaviors that cover different user groups.

Regarding the background, the participants were university students [73, 74, 76, 79, 81–83], or non-students working in the academic environment (working professionals, technical staff, and scientific staff) [69, 77, 78]. Similarly to before, examining the generalizability of the study to a larger population would be an interesting future direction.

Eye-tracking method and metrics Video oculography (VOG) is used as eye-tracking method for all experiments, as it is an invasive method that has been proven to yield better results in terms of accuracy, can capture eye movement disorders, is relatively easy to use, allows for head movements for the participants, and can be fully remote recorded. The type of eye-tracker most often employed is consisted of a remote desk mounted system with multiple cameras; however, the use of a head mounted eye-tracker was also employed in two experiments. Finally, the area of interest (AOI) is used in most of the papers and fixation metric is prevailing in most of the experiments among the several metrics measured, as shown in Table 6.

5.3 RQ2: what are the investigated phishing attack types and how do they relate to cognitive processes and brain activity?

5.3.1 Phishing and EEG

Rahman et al. (2019) [70] and Neupane et al. (2015) [69] examined website as the category of phishing attacks. In Rahman et al. (2019) [70], the research question was around which brain areas are highly activated during a phishing website detection task and what is the relationship between the brain activities and phishing detection task. In Neupane et al. (2015) [69], the authors address the question on how users behave as they process, interpret, and operationalize security information when making security decisions. In both experiments, the primary task of participants was to select whether a website shown to them is legitimate or fake. The collected brain data from the human scalp in both experiments showed that mostly the right frontal lobe and parietal lobe areas, typically involved in decision making, reasoning, and attention, are highly activated during phishing detection. Valecha et al. (2020) [71] use

Table 6 Phishing attack type and eye-tracking metrics in phishing and eye-tracking experiments. The fixation metric is the most common measured among the metrics that are identified in the experiments examined (x stands for the times a metric is found in examined experiments)

Eye-tracking metrics	Attacks via website	Attacks via email	Miscellaneous attacks
Total time spent	x		
AOI time spent	xx		
Fixations	xxxx		
Backtracking fixations	x		
AOI mean number of fixations	xx		
AOI mean number gaze duration	x		
Order of fixation	x		
AOI mean time of fixation	xx		
AOI mean time to first fixation	x		
AOI fixation duration	xx		
AOI fixation count	xx		
AOI total visit duration	x		
AOI visit count	x		
Mean fixation count		x	
Mean glance duration		x	
Saccade			x
Pupil diameter	x	x	
Heat map	x	x	

e-mail as phishing attack type. In that experiment, the primary task of subjects is to respond to a mix of phishing and benign emails or were asked to decide if the emails are genuine. The research question aims to assess the role of cognitive responses and correlated brain responses within the phishing context. The collected data showed that both the right inferior frontal and central parietal areas are responsible for adaptive decision-making and performance monitoring in phishing attacks. Finally, Hashem et al. (2017) [73] and Sun and Yeh (2017) [72] do not focus on a specific phishing attack type but approach the subject from a more general malicious activities detection angle. In their experiments, the primary task of the participants was to identify benign and malicious activity tasks, and their research attempted to answer on how user's brain processes malicious and benign activities using electroencephalogram (EEG) signals.

To summarize regarding the phishing attack types within EEG experimentation, we note that *Web-based* phishing attacks are present in two experiments, *email* in one experiment and in two experiments there was no specific phishing attack type examined but a spectrum of malicious activities is reviewed instead. Based on the factor analysis, the frontal lobe and parietal lobe areas, more dominant in decision making, reasoning, and attention, are highly activated during the phishing detection task.

5.3.2 Phishing and eye-tracking

Extending the investigation of RQ_2, in our analysis of published experiments on *Eye-tracking and phishing*, we also examined the participants' eye-tracking metrics as a response to the exposed phishing attack type.

Ramkumar et al. (2020) [74], Neupane et al. (2015) [69], Alsharnouby et al. (2015) [75], Darwish and E. Bataineh (2012) [77], Miyamoto et al. (2015) [76], Miyamoto et al. (2014) [79], and Xiong et al. (2017) [83] focused more on analyzing phishing attacks utilizing websites as means. In all experiments, the primary task of the participants was to determine whether a website was legitimate (real, safe) or fraudulent (fake, unsafe). Similarly, in Miyamoto et al. (2015) [76] and Xiong et al. (2017) [83], the participants were presented with the screenshots of a browser that rendered websites or screenshots of webpages respectively. Each one of the experiments attempted to answer a different research question: Ramkumar et al. (2020) [74] set the question of how users behave (in terms of cognitive processes involved) as they process, interpret, and operationalize security information when making a security decision, Neupane et al. (2015) [69] addressed the research question of how users process the task of detecting phishing attacks utilizing eye gaze patterns captured by an eye-tracker, Alsharnouby et al. (2015) [75] investigate which strategies the users employ to determine the legitimacy of websites, Darwish and Bataineh (2012) [77] set the research question of what the natural user viewing behavior is, when exposed to a phishing attack and Miyamoto et al. (2015) [76] evaluate the correlation between eye movements and phishing identification. Last, Xiong et al. (2017) [83] sets the question of how users allocate attention during Web page browsing.

Pfeffel et al. (2019) [78], McAlaney and P. J. Hills (2020) [80], Huang et al. (2022) [81], Yang et al. (2017) [17], and Anderson et al. (2013) [82] focused on analyzing phishing attacks involving the use of e-mails. In Pfeffel et al. (2019) [78], the participants were called to identify phishing mails versus legitimate ones and the researchers investigate on what basis did the users decide whether they are confronted with a phishing mail or a legitimate one. In McAlaney and P. J. Hills (2020) [80], the participants were shown emails that either did or did not include a phishing indicator and the research question was to identify the common elements of phishing emails that influence the victims' processing and judgment as per the email creditability. In Anderson et al. (2013) [82], the participants must distinguish among previously seen emails, novel emails, and manipulated phishing emails and the research question is how the eye movement-based memory effect influence users' susceptibility to phishing. Finally, Huang et al. (2022) [81] and Yang et al. (2017) [17] use eye-tracking method and e-mail attack as a type to verify the effectiveness of the method that is proposed in their paper.

Hashem et al. (2017) [73] did not focus on a specific phishing attack type but span their analysis across several types of malicious activities. In this experiment participants conducted usual activities as well malicious activities and the researchers investigated how the user's brain processed the malicious versus the benign activities, by means of eye-tracking while at the same time captured the spontaneous responses that may come unfiltered by the conscious mind. Towards that direction, three metrics were collected by the eye-tracker which were saccade, fixation locations, and pupil diameter.

In summary, *Website* phishing attack type is present in seven out of thirteen experiments, *e-mail* phishing appears in five experiments and study of *miscellaneous attacks* is the subject of only one experiment. In terms of the *eye-tracking metrics*, several variations were considered as shown in Table 6, with the fixation metric to be the most common one.

6 Discussion and research suggestions

The present literature survey aims to provide a systematic overview of existing experimental phishing research that leverages EEG and/or eye-tracking apparatus. Towards this direction, we examined the interlinks governing a phishing attack across the vectors through which the attack is conducted, the mediums most frequently exploited, and the technical approaches that the attackers employ to gain access to the victims' personal details. Our survey was focused on articles that contain at least one EEG-based and/or eye-tracking-based experiment within the context of a phishing attack and we analyzed a variety of montages, protocols, experimental setups as well as methods typically employed for signal preprocessing, feature engineering, and classification.

An interesting conclusion deriving from the examined literature is that the users' personality traits (e.g., attention control) may directly impact on their phishing susceptibility and suggests that users may be further trained to detect phishing attacks more effectively if they sharpen their attention control skill. In contrast, user demographics do not provide similarly conclusive indications, which in turn opens the road for further exploration on whether fully personalized model, with task/service specificity and/or with the inclusion of advanced AI-driven techniques (e.g., large language models) could be beneficial towards the development of more robust anti-phishing detection systems.

Similarly, our survey analysis indicated that focusing exclusively on either brain or gaze-driven signals analysis can yield satisfactory performant models; nonetheless, less research has been yet done in the direction of multimodal anti-phishing frameworks that combine both sources and/or when the victim is exposed to a spectrum of simultaneous phishing attacks (e.g., concurrently website, email, smishing, and vishing). In such complex scenarios, a more comprehensive investigation of the EEG and eye movement responses may reveal important insights on the ways the cortical and brain activity combined with other physiological variables interplay and relate as a response to such orchestrated attacks.

An interesting future perspective would be the investigation and validation of the findings related to these two attack types, against other types of phishing (e.g., smishing, vishing, and social media). This would also provide insights on which brainiac areas are more dominant per phishing attack type and on whether tailored cognitive models per phishing type may be needed. Similarly, another direction for further exploration relates to understanding the effect that interventional training has on the users' performance when it comes to phishing detection.

On a similar direction, the investigation of cognitive and brain responses triggered when the victim is exposed to a combination (e.g., *website* and *e-mail*) of phishing attacks and may reveal insights on how each of them affects the receiver's brain activity and respective brain lobe regions that are stimulated by such an orchestrated attack. Last, an interesting perspective for further investigation would include the concurrent employment of eye movement measurements (eye-tracking) with brain activity measures (EEG), to assess how the eye movements, cortical activity, brain activity, and other physiological variables interplay and relate as a response to the behaviors of victims of phishing (stand-alone or combination thereof) attacks.

Additionally, and as an interesting future perspective combining the best practices of the analyzed published research, we suggest a human-centric and AI-based phishing modeling approach which may provide a more comprehensive framework for identifying vulnerable users for phishing attacks (Fig. 6).

6.1 Suggestion I: multimodal anti-phishing frameworks

Current state-of-the-art anti-phishing frameworks are approaching the subject from a rather unimodal perspective and focus mainly on either gaze-based [17, 74–83] or EEG-based signal processing [70–72], to reason about the users emotional or cognitive state when experiencing a phishing attack. Despite the accuracy of such approaches, a multimodal framework that combines diverse and complementary data sources (e.g., as in [69, 73]) could be more successful to capture variations in the users' responses that are more challenging to surface when examining them in a vacuum. Such an approach can enable the development of personalized multimodal approaches, tailored per user, and usage scenario (e.g., interaction with a web-banking service), that would be (re)trained and improved every time a user interacts with the service.

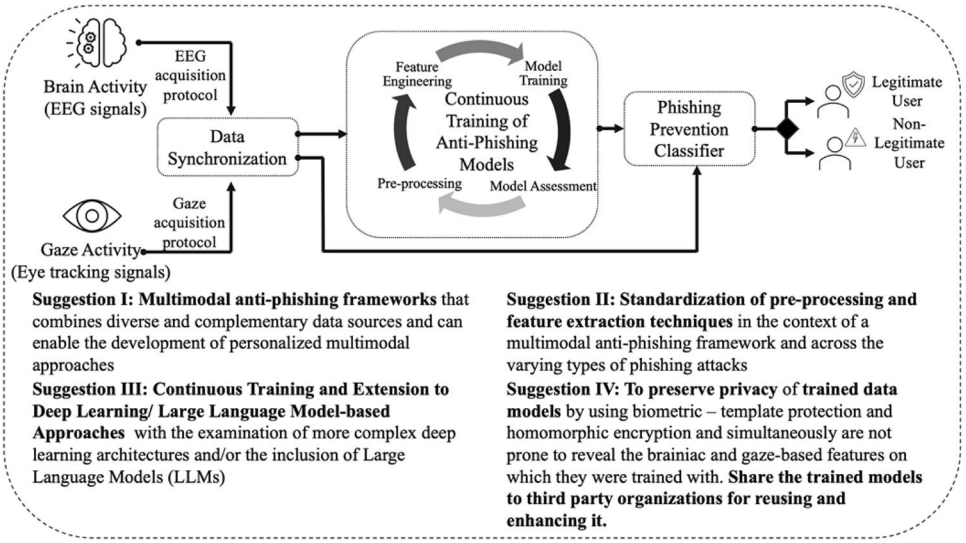

Fig. 6 Multimodal EEG and gaze-based anti-phishing framework

6.2 Suggestion II: standardization of pre-processing and feature extraction techniques

In the context of the present survey, we investigated which preprocessing methods were employed and which feature extraction methods are most applied per experimental setup. As presented in RQ_1, MATLAB toolboxes [70, 71], low-pass or high-pass filters [73], and a variety of similar proprietary software tools [69, 72] were used for this purpose. Taking into consideration these approaches and the reported results, it would be interesting to explore the effectiveness of these methods in the context of a multimodal anti-phishing framework and their robustness across the varying types of phishing attacks.

6.3 Suggestion III: continuous training and extension to deep learning/large language model-based approaches

Aiming to address RQ_1, we investigated the performance of several classification methods that are most applied in phishing experiments, with random forests and SVMs [70, 73] often scoring higher in terms of classification accuracy. Further exploration in this space, with the examination of more complex deep learning architectures and/or the inclusion of large language models (LLMs) within the training and inference processes would be another interesting direction to pursue. This could also extend to investigate whether the training on an individual basis (i.e., one model per user) can better address the conflicting conclusions from the existing research with respect to the influence the users' demographics have on their phishing susceptibility [9, 14, 20, 21] and to what degree a continuous re-training on new user input can result in more performant phishing detection systems.

6.4 Suggestion IV: privacy preservation

The combination of user-specific brainiac and gaze-based features can raise privacy concerns and for this reason biometric template protection (BTP) schemes should be considered. In this process, attention needs to be paid to enhance irreversibility (i.e., irreversible transformation over the biometric data needs to take place before these data are stored), unlikability (i.e., the stored biometric references should not be linkable across different applications or databases), and renewability (i.e., being able to issue a new template, totally different to previous ones, in case the old template is lost or compromised), while at the same time preservation in terms of verification accuracy, speed and storage requirements should be considered [86]. Moreover, self-sovereign identity (SSI) management architectures need to be further investigated aiming to provide a viable solution to the end-users for keeping control on diverse access levels to their anti-phishing models. Such a secure—in terms of privacy preservation—framework can also to facilitate the transfer of scientific knowledge to other domains and enable model sharing across diverse organizations such as governments or health and finance institutions.

In Fig. 7, we describe a brief scenario that demonstrates the usefulness and anticipated value of such an approach:

7 Conclusion

The purpose of this survey is to analyze articles that focus on conducting experiments using EEG-based (electroencephalography) and eye-tracking apparatus within a phishing context. The survey findings indicate that the most commonly studied phishing attack types were website and email

phishing. These experiments typically involved university students or academic personnel as participants and were conducted in controlled laboratory environments, which may have limited ecological validity.

The controversy observed in terms of the influence demographic factors can have in phishing susceptibility, the narrower participants' demographics, the employment of controlled experimental conditions, and the typical isolated examination of either the brain or the gaze-based signals indicate towards interesting future research directions from improved phishing detection and prevention.

More specifically, we recommend conducting additional research to explore the applicability and generalizability of these findings to other commonly encountered phishing types, such as voice or SMS phishing. Furthermore, there is a need to assess the resilience of individuals facing multiple orchestrated attacks and to simultaneously analyze eye movement and brain activity measurements. Incorporating advanced AI methods, such as complex deep learning neural networks and/or large language models, could enhance the analysis. Additionally, expanding experimental evaluations to simulate real-life unsecure operating conditions would be beneficial, as it may contribute to the development of more robust anti-phishing mechanisms.

The authors aspire that the present analysis will inspire more researchers working on the field to expand the current state-of-the-art across the three pillars outlined in Section 4 and based on the high-level framework proposed at Section 6.

7.1 Limitations

In the present survey we identified some limitations. A *first limitation* is the short number of papers found on phishing and EEG or eye-tracking apparatus. Although the original search for [Phishing] returned a fairly large number of papers dated since 2003, when the search was narrowed down to [Phishing AND EEG] and [Phishing AND Eye-tracking] only forty-two (42) papers were returned, largely skewed in terms of publication date towards the last decade (from 2012 onwards). In these 42 papers, five (5) experiments were identified related [Phishing AND EEG] and thirteen (13) experiments in the field of [Phishing AND Eye-tracking]. Our search indicated that three (3) papers approach the subject from the adjacent (to the EEG) areas of fNIRS (functional Near Infrared Spectroscopy) [87] and fMRI (functional Magnetic Resonance Imaging) [20, 88].

Another limitation is that in almost all the examined experiments, a "secure" university lab environment was used, with students constituting the most representative sample in terms of participants in the studies. This might may have impacted on the ecological validity of the experiments, since the participants are representative of more narrow demographics and may not have sensed authentic security threats due to the controlled environment. This opens the way for further exploration of the generalizability of these findings to a wider population, characterized by varying demographics and/or who may be experiencing an attack under uncontrolled (real-world) operating conditions.

Finally, the last point also extends to cover for *another limitation* related to the operation of the involved biometrics systems (EEG and eye-tracking devices). In all examined experiments, the subjects participating were measured during a single visit in a controlled (university) environment. However, to capture signals indicative of real-life phishing attacks, these biometric systems should often be employed multiple times per day, potentially every day and/or over a lengthier period. This imposes challenges as per the easiness to move the necessary equipment outside of laboratory environments to simulate real-world scenarios.

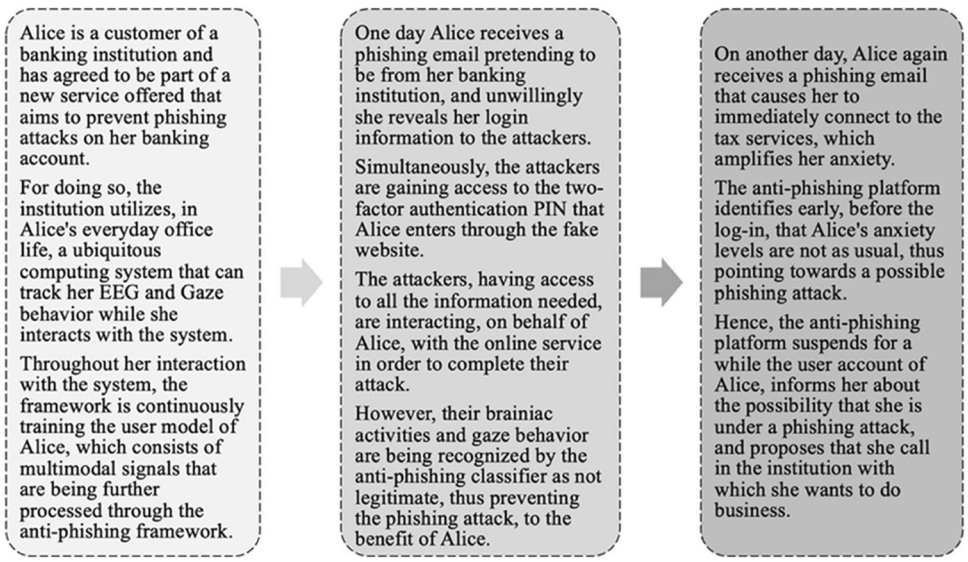

Fig. 7 User scenario that demonstrates the envisioned anti-phishing framework

Appendix

Appendix Tables 7 and 8.

Table 7 List of reviewed experimental setup in EEG and hishing papers

Paper	Number of participants	Gender	Age	Synthesis	Phishing attack type	Number of Trials	EEG device	Placement	Channels	Hz	Analyzed electrodes	Preprocessing	Feature extraction	Classification	Accuracy (%)
Neupane et al. (2015) [69]	25	16 Males	Mean 20	Students, working professionals and non-working	Websites	37	Wireless EEG sensor B-Alert headset, X10-Standard	10–20	10	256	Fz, F3, F4, C3, Cz, C4,P3, POz, P4	Proprietary software	Proprietary software	Proprietary software—QDA	69.69
Rahman et al. (2018) [70]	15	10 Males	20–32	Students	Websites	4	EMOTIV EPOC X 14 Channel Mobile Brainwear	10–20	14	N/A	AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4	MATLAB AAR, butterworth	PARAFAC2 tensor decomposition	BayesNet, logistic regression, JRip, IB1, random forest	97
Valecha et al. (2020) [71]	24	13 male	18–23	Students	E-mail	150	Curry 7 Neuroimaging Suite	10–20	64	500	N/A	MATLAB ICA	MATLAB ICA	ICA	N/A
Sun & Yeh (2017) [72]	40	20 male	Mean 23.55	Students	Reading task	N/A	MindWave Mobile	10–20	2	512	N/A	Proprietary software	Proprietary software	Proprietary software	N/A
Hashem et al. (2017) [73]	25	15 male	18–34	Students	Benign and malicious activity tasks	150	N/A	10–20	256	1000	N/A	Low-pass and high-pass filters	WPD MATLAB	SVM, k-NN, random forest, bagging predictors	99.77

Table 8 List of reviewed experimental setup in eye-tracking and phishing papers

Paper	Number of participants	Gender	Age	Synthesis	Phishing attack type	Eye-tracker	Eye-tracker type	Eye-tracker technique	Number of AOIs	Metrics
Ramkumar et al. (2020) [74]	16	2 female	Mean 22,68	Students	Website	Dikablis	Head mounted	VOG	5	Mood, score, total time spent, time spent on areas of interest, fixations, backtracking fixations, normalized pupil area, accounting for length differences in URLs
Neupane et al. (2015) [69]	25	16 male	20	Students, working professionals, and non-working	Website	EyeTech DS TM3	Remote desk mounted	VOG	3	AOI mean number of fixations, AOI mean number gaze duration
Alsharnouby et al. (2015) [75]	21	9 male	27	Students, professionals	Website	Tobii 1750	Remote desk mounted	VOG	4	Time spent on areas of interest
Miyamoto et al. (2014) [76]	23	Mainly males	20's	Students	Website	Tobii TX300	Remote desk mounted	VOG		Fixation, order of fixation
Darwish & Bataineh (2012) [77]	36	39% male	18–55 (91% 18–35)	Students, non-students	Website	Tobii T120	Remote desk mounted	VOG	4	AOI mean fixation counts, AOI mean time of fixation, AOI mean time to first fixation
Pfeffel et al. (2019) [78]	22	3 female	N/A	Technical staff, scientific staff, and students	E-mail	Tobii Pro Glasses 2	Head unit	VOG	5	AOI fixation duration, AOI fixation count, AOI total visit duration, AOI visit count
Miyamoto et al. (2015) [79]	23	Majority male	20's	Students	Website	Tobii TX300	Remote desk mounted	VOG	4	Number and duration of fixations in AOI
McAlaney & Hills, (2020) [80]	22	90% female	Mean age 20.9	Students	E-mail	SMI RED 500	Remote desk mounted	VOG	6	Total dwell time, mean fixation count, number of regressions, mean glance duration, entry time and entry sequence
Hashem et al., (2017) [73]	25	15 male	18–34	Students	Activities	Tobii Pro X2-60	Remote desk mounted	VOG		Saccade, fixation locations, pupil diameter

Table 8 (continued)

Paper	Number of participants	Gender	Age	Synthesis	Phishing attack type	Eye-tracker	Eye-tracker type	Eye-tracker technique	Number of AOIs	Metrics
Huang et al. (2022) [81]	160	N/A	N/A	Students	E-mail	Tobii Pro T60XL	Remote desk mounted	VOG	13	Pupil diameters
Yang et al. (2022) [17]	50	50% male	20–30	Students, non-students	E-mail	N/A	N/A	VOG	1	Gaze time, number of gazes
Anderson et al. (2013) [82]	45	N/A	N/A	Students	E-mail	Tobii T120	Remote desk mounted	VOG		Heat map
Xiong et al. (2017) [83]	32	10 female	Mean age 19	Students	Webpage snapshots	EyeLink 1000Plus	Remote desk mounted	VOG	1	Number of fixations, mean fixation duration, visits, heat maps

Funding Open access funding provided by HEAL-Link Greece. This work has been financially supported by the Hellenic Foundation for Research & Innovation (HFRI) under the 2nd Call for proposals for H.F.R.I. Research Projects to Support Faculty Members and Researchers, under the project entitled Electroencephalography and Eye Gaze driven Framework for Intelligent and Real-Time Human Cognitive Modelling (CogniX) with Proposal ID 3849.

Data availability No datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Basit A, Zafar M, Liu X, Javed AR, Jalil Z, Kifayat K (2021) A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun Syst 76(1):139–154. https://doi.org/10.1007/s11235-020-00733-2
2. Kaloudi N, Li J (2021) The AI-based cyber threat landscape: a survey. ACM Comput Surv 53(1):1–34. https://doi.org/10.1145/3372823
3. Montañez R, Golob E, Xu S (2020) Human cognition through the lens of social engineering cyberattacks. Front Psychol 11:1755. https://doi.org/10.3389/fpsyg.2020.01755
4. Hakim ZM et al (2021) The phishing email suspicion test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behav Res 53(3):1342–1352. https://doi.org/10.3758/s13428-020-01495-0
5. Anti Phishing Working Group (APWG) (2022) Phishing activity trends report, 1st Quarter, https://www.docs.apwg.org/. Accessed 17 Jan 2023
6. Jari M (2022) An overview of phishing victimization: Human factors, training and the role of emotions. In: Computer science and information technology. 12th International Conference on Computer Science and Information Technology (CCSIT 2022). Academy and Industry Research Collaboration Center (AIRCC). https://doi.org/10.5121/csit.2022.121319
7. Almoqbil A, O'Connor B, Anderson R, Shittu J, McLeod P (2021) Modeling deception: A case study of email phishing. In: Proceedings from the Document Academy (Vol. 8, Issue 2). Document Academy. https://doi.org/10.35492/docam/8/2/8
8. Chan-Tin E, Stalans L, Johnston S, Reyes D, Kennison S (2022) Predicting phishing victimization. In: Fifth international workshop on systems and network telemetry and analytics. HPDC '22: The 31st International Symposium on High-Performance Parallel and Distributed Computing. ACM. https://doi.org/10.1145/3526064.3534107

9. Ge Y, Lu L, Cui X, Chen Z, Qu W (2021) How personal characteristics impact phishing susceptibility: the mediating role of mail processing. Appl Ergon 97:103526. https://doi.org/10.1016/j.apergo.2021.103526
10. Sabir B, Ullah F, Babar MA, Gaire R (2022) Machine learning for detecting data exfiltration: a review. ACM Comput Surv 54(3):1–47. https://doi.org/10.1145/3442181
11. Tomaselli J, Willoughby A, Amezcua JV, Delehanty E, Floyd K, Wright D, Lammers M, Vetter R (2021) Verifying phishmon. In: Proceedings of the 2021 ACM Southeast Conference. ACM SE '21: 2021 ACM Southeast Conference. ACM. https://doi.org/10.1145/3409334.3452082
12. Peng T, Harris I, Sawa Y (2018) Detecting phishing attacks using natural language processing and machine learning. In: 2018 IEEE 12th International Conference on Semantic Computing (ICSC). IEEE. https://doi.org/10.1109/icsc.2018.00056
13. Jain AK, Gupta BB (2018) PHISH-SAFE: URL Features-based phishing detection system using machine learning. In: Advances in Intelligent Systems and Computing. Springer Singapore. pp 467–474. https://doi.org/10.1007/978-981-10-8536-9_44
14. Lin T et al (2019) Susceptibility to spear-phishing emails: effects of internet user demographics and email content. ACM Trans Comput-Hum Interact 26(5):1–28. https://doi.org/10.1145/3336141
15. Fasllija E, Enişer HF, Prünster B (2019) Phish-Hook: Detecting phishing certificates using certificate transparency logs. In: Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering. Springer International Publishing. pp 320–334. https://doi.org/10.1007/978-3-030-37231-6_18
16. Althobaiti K, Meng N, Vaniea K (2021) I don't need an expert! making url phishing features human comprehensible. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. CHI '21: CHI Conference on Human Factors in Computing Systems. ACM. https://doi.org/10.1145/3411764.3445574
17. Yang J, Yang P, Jin X, Ma Q (2017) Multi-classification for malicious url based on improved semi-supervised algorithm. In: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). https://doi.org/10.1109/cse-euc.2017.34
18. Althobaiti K, Vaniea K, Zheng S (2018) Faheem: Explaining URLs to people using a Slack bot. In: Symposium on Digital Behaviour Intervention for Cyber Security. pp 1–8 http://aisb2018.csc.liv.ac.uk/PROCEEDINGS%20AISB2018/Digital%20Behaviour%20Interventions%20for%20CyberSecurity%20-%20AISB2018.pdf#page=8
19. Volkamer M, Renaud K, Reinheimer B, Kunz A (2017) User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. Comput Secur 71:100–113. https://doi.org/10.1016/j.cose.2017.02.004
20. Neupane A, Saxena N, Maximo JO, Kana R (2016) Neural markers of cybersecurity: an fMRI study of phishing and malware warnings. IEEE Trans Inform Forensic Secur 11(9):1970–1983. https://doi.org/10.1109/TIFS.2016.2566265
21. Halevi T, Memon N, Nov O (2015) Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. SSRN J. https://doi.org/10.2139/ssrn.2544742
22. Iuga C, Nurse JRC, Erola A (2016) Baiting the hook: factors impacting susceptibility to phishing attacks. In: Human-centric Computing and Information Sciences (Vol. 6, Issue 1). Springer Science and Business Media LLC. https://doi.org/10.1186/s13673-016-0065-2
23. Jagatic TN, Johnson NA, Jakobsson M, Menczer F (2007) Social phishing. Commun ACM 50(10):94–100. https://doi.org/10.1145/1290958.1290968
24. Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J (2010) Who falls for phish? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '10: CHI Conference on Human Factors in Computing Systems. ACM. https://doi.org/10.1145/1753326.1753383
25. Robinson L, Schulz J, Blank G, Ragnedda M, Ono H, Hogan B, Mesch GS, Cotten SR, Kretchmer SB, Hale TM, Drabowicz T, Yan P, Wellman B, Harper M-G, Quan-Haase A, Dunn HS, Casilli AA, Tubaro P, Carvath R, Khilnani A (2020) Digital inequalities 2.0: Legacy inequalities in the information age. In: First Monday. University of Illinois Libraries. https://doi.org/10.5210/fm.v25i7.10842
26. Paper, Research & Liu, Zhihui & Zhou, Lina & Zhang, Dongsong. (2021). Effects of Demographic Factors on Phishing Victimization in the Workplace
27. Sun JC-Y, Yu S-J, Lin SSJ, Tseng S-S (2016) The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. Comput Hum Behav 59:249–257. https://doi.org/10.1016/j.chb.2016.02.004
28. Butavicius, M.A., Parsons, K., Pattinson, M.R., McCormac, A., Calic, D., & Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. International Symposium on Human Aspects of Information Security and Assurance
29. Rocha Flores W, Holm H, Svensson G, Ericsson G (2014) Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Inf Manag Comput Secur 22(4):393–406. https://doi.org/10.1108/IMCS-11-2013-0083
30. Mohebzada JG, Zarka AE, Bhojani AH, Darwish A (2012) Phishing in a university community: Two large scale phishing experiments. In: 2012 International Conference on Innovations in Information Technology (IIT). https://doi.org/10.1109/innovations.2012.6207742
31. Oliveira D, Rocha H, Yang H, Ellis D, Dommaraju S, Muradoglu M, Weir D, Soliman A, Lin T, Ebner N (2017) Dissecting Spear Phishing Emails for Older vs Young Adults. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. CHI '17: CHI Conference on Human Factors in Computing Systems. ACM. https://doi.org/10.1145/3025453.3025831
32. Diaz A, Sherman AT, Joshi A (2020) Phishing in an academic community: a study of user susceptibility and behavior. Cryptologia 44(1):53–67. https://doi.org/10.1080/01611194.2019.162334
33. Wash R (2020) How experts detect phishing scam emails. Proc ACM Hum -Comput Interact 4(CSCW2):1–28. https://doi.org/10.1145/3415231
34. Jones HS, Towse JN, Race N, Harrison T (2019) Email fraud: the search for psychological predictors of susceptibility. PLoS ONE 14(1):e0209684. https://doi.org/10.1371/journal.pone.0209684
35. Neupane A, Satvat K, Saxena N, Stavrinos D, Bishop, HJ (2018) Do social disorders facilitate social engineering? In: Proceedings of the 34th Annual Computer Security Applications Conference. ACSAC '18: 2018 Annual Computer Security Applications Conference. ACM. https://doi.org/10.1145/3274694.3274730
36. Blythe M, Petrie H, Clark JA (2011) F for fake. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '11: CHI Conference on Human Factors in Computing Systems. ACM. https://doi.org/10.1145/1978942.1979459
37. Canova G, Volkamer M, Bergmann C, Reinheimer B (2015) NoPhish App Evaluation: Lab and Retention Study. In: Proceedings 2015 Workshop on Usable Security. Workshop on Usable

Security. Internet Society. https://doi.org/10.14722/usec.2015.23009
38. Siadati H, Palka, S, Siegel A, McCoy, D (2017) Measuring the effectiveness of embedded phishing exercises
39. Caputo DD, Pfleeger SL, Freeman JD, Johnson ME (2014) Going spear phishing: exploring embedded training and awareness. IEEE Secur Privacy 12(1):28–38. https://doi.org/10.1109/MSP.2013.106
40. Higashino M (2019) A design of an anti-phishing training system collaborated with multiple organizations. In: Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services. iiWAS2019: The 21st International Conference on Information Integration and Web-based Applications & Services. ACM. https://doi.org/10.1145/3366030.3366086
41. JalalyBidgoly A, JalalyBidgoly H, Arezoumand Z (2020) A survey on methods and challenges in EEG based authentication. Computers Sec 93:101788. https://doi.org/10.1016/j.cose.2020.101788
42. Katsini C, Abdrabou Y, Raptis GE, Khamis M, Alt F (2020) The role of eye gaze in security and privacy applications: Survey and future HCI Research Directions. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376840
43. Hari Singh, Dr. Jaswinder Singh (2012) Human eye tracking and related issues: a review. Int J Scientific Res Pub 2(9)
44. Khonji M, Iraqi Y, Jones A (2013) Phishing detection: a literature survey. IEEE Commun Surv Tutorials 15(4):2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009
45. Abdillah R, Shukur Z, Mohd M, Ts M, Murah Z (2022) Phishing classification techniques: a systematic literature review. IEEE Access 10:41574–41591. https://doi.org/10.1109/ACCESS.2022.3166474
46. Alabdan R (2020) Phishing attacks survey: types, vectors, and technical approaches. Future Internet 12(10):168. https://doi.org/10.3390/fi12100168
47. Aleroud A, Zhou L (2017) Phishing environments, techniques, and countermeasures: a survey. Comput Secur 68:160–196. https://doi.org/10.1016/j.cose.2017.04.006
48. Stavroulakis P, Stamp M, Eds. (2010) *Handbook of information and communication security*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04117-4
49. Das A, Baki S, El Aassal A, Verma R, Dunbar A (2020) SoK: a comprehensive reexamination of phishing research from the security perspective. IEEE Commun Surv Tutorials 22(1):671–708. https://doi.org/10.1109/COMST.2019.2957750
50. Rader MA, M. Rahman S. (Shawon) (2013) Phishing Techniques and Mitigating the Associated Security Risks. In International Journal of Network Security & Its Applications. Academy and Industry Research Collaboration Center (AIRCC). 5(4):23–41. https://doi.org/10.5121/ijnsa.2013.5402
51. Phishing.org. Phishing Organization, https://www.phishing.org/history-of-phishing, Accessed 17 Jan 2023
52. Verizon Com. Data Breach Investigation Report (2022) https://www.verizon.com/business/resources/Td4c/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
53. Anti Phishing Working Group (APWG) Phishing activity trends report, 3rd quarter 2022, https://docs.apwg.org/, Accessed 17 Jan 2023
54. UK Government, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022, Accessed 25 Jan 2023
55. Chiew KL, Yong KSC, Tan CL (2018) A survey of phishing attacks: their types, vectors and technical approaches. Expert Syst Appl 106:1–20. https://doi.org/10.1016/j.eswa.2018.03.050
56. İnce R, Adanır SS, Sevmez F (2021) The inventor of electroencephalography (EEG): Hans Berger (1873–1941). Childs Nerv Syst 37(9):2723–2724. https://doi.org/10.1007/s00381-020-04564-z
57. Bonci A, Fiori S, Higashi H, Tanaka T, Verdini F (2021) An introductory tutorial on brain–computer interfaces and their applications. Electronics 10(5):560. https://doi.org/10.3390/electronics10050560
58. Di Flumeri G, Aricò P, Borghini G, Sciaraffa N, Di Florio A, Babiloni F (2019) The dry revolution: evaluation of three different EEG dry electrode types in terms of signal spectral features, mental states classification and usability. Sensors 19(6):1365. https://doi.org/10.3390/s19061365
59. Mecarelli O (2019) Electrode placement systems and montages. In: Clinical Electroencephalography. Springer International Publishing. pp 35–52. https://doi.org/10.1007/978-3-030-04573-9_4
60. Oostenveld R, Praamstra P (2001) The five percent electrode system for high-resolution EEG and ERP measurements. Clin Neurophysiol 112(4):713–719. https://doi.org/10.1016/S1388-2457(00)00527-7
61. Hu L, Zhang Z (2020) Evolving EEG signal processing techniques in the age of artificial intelligence. Brain Science Adv 6(3):159–161. https://doi.org/10.26599/BSA.2020.9050027
62. Wan X et al (2019) A review on electroencephalogram based brain computer interface for elderly disabled. IEEE Access 7:36380–36387. https://doi.org/10.1109/ACCESS.2019.2903235
63. Klaib AF, Alsrehin NO, Melhem WY, Bashtawi HO, Magableh AA (2021) Eye tracking algorithms, techniques, tools, and applications with an emphasis on machine learning and Internet of Things technologies. Expert Syst Appl 166:114037. https://doi.org/10.1016/j.eswa.2020.114037
64. Carter BT, Luke SG (2020) Best practices in eye tracking research. Int J Psychophysiol 155:49–62. https://doi.org/10.1016/j.ijpsycho.2020.05.010
65. Punde PA, Jadhav ME, Manza RR (2017) A study of eye tracking technology and its applications. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM). IEEE. https://doi.org/10.1109/icisim.2017.8122153
66. Sarkar A, Sanyal G, Majumder S (2017) Performance evaluation of an eye tracking system under varying conditions. IJCSNS 17(4):182–191
67. Joseph AW, Murugesh R (2020) Potential Eye Tracking Metrics and Indicators to Measure Cognitive Load in Human-Computer Interaction Research. In Journal of scientific research. Banaras Hindu University. 64(1):168–175. https://doi.org/10.37398/jsr.2020.640137
68. Moher D, Liberati A, Tetzlaff J, Altman DG (2010) Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Int J Surg 8(5):336–341. https://doi.org/10.1016/j.ijsu.2010.02.007
69. Neupane A, Rahman Md. L, Saxena N, Hirshfield L (2015) A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. CCS'15: The 22nd ACM Conference on Computer and Communications Security. ACM. https://doi.org/10.1145/2810103.2813660
70. Rahman Md. L, Bardhan S, Neupane A, Papalexakis E, Song C (2019) Learning tensor-based representations from brain-computer interface data for cybersecurity. In: Machine learning and knowledge discovery in databases. Springer International Publishing. pp 389–404. https://doi.org/10.1007/978-3-030-10997-4_24
71. Valecha R, Gonzalez A, Mock J, Golob EJ, Raghav Rao H (2019) Investigating Phishing Susceptibility—An Analysis of Neural Measures. In: Information Systems and Neuroscience. Springer International Publishing. pp 111–119. https://doi.org/10.1007/978-3-030-28144-1_12

72. Sun JC-Y, Yeh KP-C (2017) The effects of attention monitoring with EEG biofeedback on university students' attention and self-efficacy: the case of anti-phishing instructional materials. Comput Educ 106:73–82. https://doi.org/10.1016/j.compedu.2016.12.003
73. Hashem Y, Takabi H, Dantu R, Nielsen R (2017) A Multi-Modal Neuro-Physiological Study of Malicious Insider Threats. In: Proceedings of the 2017 International Workshop on Managing Insider Security Threats. CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM. https://doi.org/10.1145/3139923.3139930
74. Ramkumar N, Kothari V, Mills C, Koppel R, Blythe J, Smith S, Kun AL (2020) Eyes on URLs: Relating Visual Behavior to Safety Decisions. In: ACM Symposium on Eye Tracking Research and Applications. ETRA '20: 2020 Symposium on Eye Tracking Research and Applications. ACM. https://doi.org/10.1145/3379155.3391328
75. Alsharnouby M, Alaca F, Chiasson S (2015) Why phishing still works: user strategies for combating phishing attacks. Int J Hum Comput Stud 82:69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005
76. Miyamoto D, Blanc G, Kadobayashi Y (2015) Eye Can Tell: On the correlation between eye movement and phishing identification. International Conference on Neural Information Processing
77. Darwish A, Bataineh E (2012) Eye tracking analysis of browser security indicators. In: 2012 International Conference on Computer Systems and Industrial Informatics. 2012 International Conference on Computer Systems and Industrial Informatics (ICCSII). IEEE. https://doi.org/10.1109/iccsii.2012.6454330
78. Pfeffel K, Ulsamer P, Müller NH (2019) Where the user does look when reading phishing mails – An Eye-Tracking Study. In: Learning and collaboration technologies. Designing learning experiences. Springer International Publishing. pp 277–287. https://doi.org/10.1007/978-3-030-21814-0_21
79. Miyamoto D, Iimura T, Blanc G, Tazaki H, Kadobayashi Y (2014) EyeBit: Eye-tracking approach for enforcing phishing prevention habits. In: 2014 third international workshop on building analysis datasets and gathering experience returns for security (BADGERS). https://doi.org/10.1109/badgers.2014.14
80. McAlaney J, Hills PJ (2020) Understanding phishing email processing and perceived trustworthiness through eye tracking. Front Psychol 11:1756. https://doi.org/10.3389/fpsyg.2020.01756
81. Huang L, Jia S, Balcetis E, Zhu Q (2022) ADVERT: an adaptive and data-driven attention enhancement mechanism for phishing prevention. IEEE Trans Inform Forensic Secur 17:2585–2597. https://doi.org/10.1109/TIFS.2022.3189530
82. Anderson B, Vance A, Eargle D (2013) Is your susceptibility to phishing dependent on your memory?. WISP 2012 Proceedings. p 40. https://aisel.aisnet.org/wisp2012/40
83. Xiong A, Proctor RW, Yang W, Li N (2017) Is domain highlighting actually helpful in identifying phishing web pages? Hum Factors 59(4):640–660. https://doi.org/10.1177/0018720816684064
84. Nunez PL et al (1997) EEG coherency. Electroencephalogr Clin Neurophysiol 103(5):499–515. https://doi.org/10.1016/S0013-4694(97)00066-7
85. Wang J, Wang M (2021) Review of the emotional feature extraction and classification using EEG signals. Cognitive Robotics 1:29–40. https://doi.org/10.1016/j.cogr.2021.04.001
86. Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017) Multi-biometric template protection based on homomorphic encryption. Pattern Recogn 67:149–163. https://doi.org/10.1016/j.patcog.2017.01.024
87. Neupane A, Saxena N, Hirshfield L (2017) Neural underpinnings of website legitimacy and familiarity detection. In: Proceedings of the 26th International Conference on World Wide Web. WWW '17: 26th International World Wide Web Conference. International World Wide Web Conferences Steering Committee. https://doi.org/10.1145/3038912.3052702
88. Neupane A, Saxena N, Kuruvilla K, Georgescu M, Kana R (2014) Neural signatures of user-centered security: An fMRI study of phishing, and malware warnings. In: Proceedings 2014 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium. Internet Society. https://doi.org/10.14722/ndss.2014.23056