Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study

Fauzan Prasetyo Eka Putra[1*], Ubaidi[2], Achmad Zulfikri[3], Goffal Arifin[4], Revi Mario Ilhamsyah[5]
[1,2,3,4,5]Fakultas Teknik, Informatika Universitas Madura Jl. Raya Panglegur No.Km 3,5, Barat, Panglegur, Kec. Tlanakan, Kabupaten Pamekasan, Jawa Timur 69371
[1]prasetyo@unira.ac.id, [2]ubed@unira.ac.id, [3]achamadzulfikri20@gmail.com, [4]goffalarifin09@gmail.com, [5]revimarioilhamsyah@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 21-07-2024
Accepted: 22-07-2024
Published: 09-08-2024

Keywords:
Analysis; Trends; Phishing Attack; Impact; Prevention.

ABSTRACT

Phishing is a growing form of cybercrime that poses a serious threat to information security in the digital world. This article aims to analyze the latest trends in phishing attacks and evaluate effective prevention methods. Using data from cybersecurity reports, case studies, and academic literature, this research identifies the latest phishing techniques such as spear phishing, whaling, and smishing that are increasingly sophisticated and difficult to detect. The analysis showed that while anti-phishing technologies such as email filters, two-factor authentication (2FA), and encryption have undergone significant developments, user awareness and education remain key factors in preventing phishing attacks. Additionally, strict policies and procedures at the organizational level also play an important role in reducing risk. The case studies presented in this article demonstrate the successful implementation of various prevention methods in several organizations, although challenges in terms of technology adoption and user training remain. For example, spear phishing and whaling have been effectively countered by tailored training programs and advanced threat detection systems. The article concludes by providing practical recommendations to increase user awareness and strengthen organizational policies to protect against phishing attacks. It also includes foresight to illustrate the possible evolution of phishing attacks, emphasizing the need for continuous innovation in cyber defense strategies. This comprehensive approach underscores the importance of a multi-layered defense system that combines technological solutions with human vigilance to effectively combat the ever-evolving threat of phishing.

INTRODUCTION

The development of technology in today's digital era has experienced a tremendous surge from year to year. Various types of information technology in digital form are now an integral part of the daily life of the global community, including the internet. The internet has facilitated the emergence of various applications that can be utilised by computer users to communicate, search for information, and do business. This advancement in information and communication technology clearly drives the trend of global technological development with all forms of human creativity. This development is increasingly expanding into various fields, allowing people to quickly access the information they need anytime and anywhere. Today, almost a third of the world's population uses the internet in their daily lives, indicating how important it is in modern life.

However, this technological advancement is not free from a number of challenges and problems, including a crime known as Cyber Crime. The increasing use of technology also increases the vulnerability to various types of crimes committed by irresponsible individuals, such as fraud, theft, defamation, and various other crimes committed through the internet. One of the most commonly encountered forms of crime that harms many parties is phishing attacks.

Phishing is a form of cybercrime where the perpetrator attempts to obtain sensitive information such as usernames, passwords, and other information by posing as a trusted entity in electronic communications. Phishing is often carried out through fake, official-looking emails, text messages or websites. The goal is to trick victims into voluntarily providing their personal information. In recent years, phishing has become a serious threat in the digital world, especially with the increase in online activity causing the number of phishing attacks to increase significantly. Phishing not only targets individuals, but also large corporations, financial institutions, and government organisations. Phishing techniques are constantly evolving to become more sophisticated and difficult to recognise. Perpetrators often use social engineering techniques to make their messages seem more convincing, such as personalising emails and using logos and website layouts that closely resemble the original(Ardiyanti, n.d.).

Phishing attacks can cause huge financial losses to victims. In addition to losing money, victims can also suffer damage to their reputation and trust, both individually and organisationally. With the development of technologies such

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

as artificial intelligence and automation, phishing attacks are becoming easier to carry out and harder to detect and stop. Many internet users still lack awareness of the dangers of phishing and are not adequately trained to recognise the warning signs of these attacks, making them more vulnerable to becoming victims. Due to its detrimental impact, phishing has become a major focus of cybersecurity improvement efforts. Identifying the latest trends in phishing attacks and developing effective prevention methods are important steps to protect individuals and organisations from this threat.

This article aims to analyse phishing attack trends, identifying and assessing the latest phishing techniques used by cybercriminals. The article will cover the evolution of attack methods, emerging patterns, as well as different types of phishing such as spear phishing, whaling, and smishing. Spear phishing is an attack targeted at a specific individual or organisation using personalised information to increase the effectiveness of the attack. Whaling is a type of spear phishing that targets high-profile individuals such as corporate executives or government officials. Smishing, or SMS phishing, is a type of phishing that uses text messages to deceive victims.

In addition, this article also aims to evaluate effective prevention methods by assessing the various approaches and technologies that have been developed to prevent phishing attacks. This research will discuss the effectiveness of email filters, two-factor authentication (2FA), encryption, and the role of user education and training in preventing phishing. Email filters can help filter out suspicious messages before they reach a user's inbox. Two-factor authentication (2FA) adds an additional layer of security by requiring users to verify their identity through a method other than a password. Encryption helps protect sensitive data during transmission. User education and training is essential to raise awareness of the dangers of phishing and how to recognise the signs of an attack.

In addition, this article also aims to evaluate effective prevention methods by assessing the various approaches and technologies that have been developed to prevent phishing attacks. This research will discuss the effectiveness of email filters, two-factor authentication (2FA), encryption, and the role of user education and training in preventing phishing. Email filters can help filter out suspicious messages before they reach a user's inbox. Two-factor authentication (2FA) adds an additional layer of security by requiring users to verify their identity through a method other than a password. Encryption helps protect sensitive data during transmission. User education and training is essential to raise awareness of the dangers of phishing and how to recognise the signs of an attack(Yani, 2016).

LITERATURE REVIEW

A number of previous research studies have discussed the various threats of phishing attacks carried out against a number of individuals or groups or organisations.
The following are previous research studies:

1. (Wijoyo et al., n.d.)This research discusses the various forms and types of phishing attacks, such as email, SMS, phone calls, web phishing, and pop-ups, The types of phishing discussed include scam phishing, blind phishing, spear phishing, clone phishing, whaling, vishing, pharming, and smishing, all of which aim to obtain sensitive information or financial gain. this research also discusses the characteristics and preventive measures to avoid phishing attacks, This journal provides a comprehensive guide to recognising and protecting yourself from phishing attacks in cyberspace.
2. (Radiansyah & Priyadi, 2016)In this study, the objectives carried out are to determine the factors that cause the emergence of phishing and the prevention of phishing threats. phishing and prevention of phishing threats, using the Systematic Literature Review Method to find answers to these research questions by searching for studies related to phishing. This research explains the factors that cause phishing attacks where one of them is minimal user knowledge, and also explains the various prevention of phishing so as not to harm users.
3. (Danuri, n.d.)This research discusses the development of information and communication technology in Indonesia from year to year until now, including the increasing use of the internet for socialisation and business. It also highlights the negative impacts of cybercrime, such as phishing threats, threats to the country's social, economic and defence systems. The government's efforts in establishing laws and information technology ethics education in universities are also discussed as steps to reduce cybercrime and improve information technology security in the future.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

METHOD

Figure 1. Research steps

Figure 1 explains the steps in the research method which aims to describe a stage in the research to facilitate researchers in carrying out research in an orderly and structured manner.

Literature Study

The literature study was conducted by tracing the research subject through scientific journals and previous studies that discuss issues regarding the threat of phishing attacks to support this research. Literature study involves a series of actions such as reading and recording, managing research materials from sources that are still related to this research. The data used comes from references read by the author, which are in accordance with the subject from various relevant journals. Furthermore, the data that has been obtained will be analysed using descriptive analysis.

Data Collection

In this research, data collection is done by collecting data that supports the research being conducted. Data collection was carried out after conducting a literature review of relevant previous studies on Phishing Attack Trends and Prevention Methods. The data obtained from this literature review was then collected. After the data is collected, further discussion and review of Phishing Attack Trends and Prevention is conducted.

Data Analysis

After the data was obtained and collected, the next step was to analyse the data. Data analysis was conducted qualitatively to evaluate and review phishing trends and prevention methods. Descriptive analysis is used to describe the data that has been collected. This research uses appropriate and suitable analysis methods so that the discussion generated from the data that has been collected can be relied upon and accounted for(Kurniawan, 2024).

RESULT

Phishing is one of the most common and damaging forms of cybercrime, and has undergone a significant evolution since it first emerged in the 1990s. When it first emerged in the 1990s, phishing was known as a simple yet effective fraud technique. Early attacks were typically carried out via emails that mimicked messages from financial institutions or popular online services. These emails often asked recipients to update their account information by clicking on a link that redirected them to a fake website designed to resemble the original site.

In the 2000s, phishing techniques became increasingly sophisticated by utilising social engineering. Perpetrators began customising their emails with more specific personal information, making the messages appear more convincing.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

During this period, spear phishing attacks emerged that targeted specific individuals or organisations with more relevant information and were difficult to recognise as fraudulent.

Phishing further evolved in the 2010s with methods such as spear phishing that targeted specific individuals and whaling that targeted high-level executives. Smishing and vishing techniques also came into use, tricking victims through text messages and voice calls.

Phishing has become more difficult in the 2020s due to the use of social media and multi-vector attacks that combine various methods such as email, text messages, and social media platforms. Perpetrators have also started using artificial intelligence (AI) to create more lookalike phishing emails and automate large-scale attacks(Candiwan, 2016).

The following table shows the evolution of phishing:

Table 1. Evolution of Phishing

Decade	Description
1990s	Early phishing attacks began, primarily using simple email scams pretending to be from financial institutions or popular online services, redirecting users to fake websites to steal credentials.
2000s	Phishing techniques became more sophisticated, incorporating social engineering. Spear phishing emerged, targeting specific individuals or organizations with personalized emails to increase effectiveness.
2010s	Introduction of advanced techniques like spear phishing and whaling, targeting high-level executives. Smishing (SMS phishing) and vishing (voice phishing) also gained prominence.
2020s	Phishing evolved with the use of social media for multi-vector attacks, combining email, text messages, and social media platforms. Attackers began using artificial intelligence (AI) to create more realistic phishing emails and automate large-scale attacks.

Table 1 shows an evolution of phishing from several decades to the present, the phishing evolution data is taken from website sources such as PhishingBox and Inspired eLearning, which provide detailed analyses of the evolution and impact of phishing techniques over the decades.

Phishing continues to evolve with new techniques that are increasingly sophisticated and difficult to spot. Here are some of the latest phishing attack trends to watch out for:

1. Spear Phishing

Comes from the word ‘spear’ which means spear, similar to fishing techniques that use spears to select certain fish. These attacks are targeted at specific groups, such as government officials, specific companies, or specific individuals. Spear phishing attacks are usually carried out to break into and access specialised databases that contain important information, confidential files, or financial data. Most people are unaware of this technique, as it is very well done. Attackers change the way they communicate to match their target's characteristics, occupation, and contact list to make their attacks invisible or harder to detect. Today's spear phishing attacks are getting more sophisticated by utilising information from sources such as social media to increase the likelihood of an attack.

2. Whaling

The word Whaling comes from the English word whale, which means whale. Still related to fishing, this type of phishing targets large victims or individuals who are not ordinary people. Whaling usually targets high-level executives or well-known figures, such as company directors, with the aim of disrupting their company. This attack is usually carried out by posing as one of the company's staff or by sending announcements via email messages or social media regarding the company's internal situation(Aptika dan IKP et al., n.d.).

3. Vishing

This type of phishing is done by making voice calls to phishing victims. there are various ways that fraudsters use these voice calls to carry out fraudulent attacks. usually these attacks often take advantage of a sense of urgency or fear to manipulate victims, for example, fraudsters make phone calls to victims by saying that there are victims' families who are arrested by the police, or accidents and other modes, and in the end will ask the victim for a sum of money. fraudsters usually use invalid or unknown numbers to hide their identity.

4. Smishing

Similar to Vishing, Smishing also carries out fraudulent attacks by utilising fear to manipulate victims. the difference is that in smishing, the perpetrators carry out various scams by sending text messages as if they are official from institutions or companies with the same goal, manipulating victims to do something. the mode used is usually convincing victims that they have won a lottery, lottery and the like by getting a fantastic amount of money(Ariadi et al., 2023).

5. Social Media-Based Phishing

Social media platforms such as Facebook, Twitter, LinkedIn and Instagram are increasingly being used for phishing attacks. Attackers may share phishing links or messages that appear to be from trusted contacts. In addition,

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

they will create fake profiles to establish a relationship with the victim and gain trust before launching the attack.

6. Deepfake AI

In today's digital era, Technology is growing, many technologies are being created and developed including AI, This type of Phishing utilises AI technology to create fake videos or audio that is very convincing and is starting to be used in phishing attacks. Attackers can create a fake video or voice recording that looks like it's coming from a co-worker or boss, and then ask the victim to perform certain actions such as transferring money or providing the victim's personal information(Nur'adila, n.d.).

7. Scam Phishing

This is a type of phishing scam that cybercriminal attackers use to trick their victims into providing personal information, such as bank account numbers, account passwords, and other important card numbers. They usually send modified links or files that contain malware. The information obtained is then used to hack into our accounts, steal money, and commit other crimes. usually the media that is often used includes sms, email, telephone, or social media.

8. Cloning and Blind Phishing

Phishing clone technique is done by cloning the original website in order to attract and trick users. In this phishing technique, the perpetrator will ask the victim to input their personal information in the input field on the fake website that has been provided by the perpetrator, which in the end the victim will be directed to the original website and without realising that the victim has become a victim of this phishing clone, and Blind Phishing is the most common type of phishing that occurs and is used. blind phishing is similar to blind phishing, where the attacker sends phishing messages en masse without targeting specific individuals or organisations. In blind phishing, there is no specific target and the attacker usually uses broad dissemination techniques such as sending emails or text messages to a large number of people in the hope that some recipients will fall for it(Nugroho1 et al., n.d.).

DISCUSSION

Impact of Phishing Attacks

There are even more risks to personal data protection in the rapidly evolving digital age caused by phishing crimes. These phishing crimes are extremely dangerous threats and influences that can jeopardise a person's safety. Victim of this crime can experience a number of devastating effects, such as:

1. Loss of account or personal data

The impact of phishing is the loss of personal account access which can result in the loss of important data, and other important personal information belonging to the victim. Phishing often leads to the theft of personal data, including financial information and login credentials. This can lead to the victim's identity being used for various other forms of crime.

2. Damage the reputation of an individual or company

The impact of this phishing attack is also the financial loss of the company and also the loss of important company data, so it can damage the company's reputation. companies that are victims of phishing attacks can experience severe reputational damage, which adversely affects trust in the sustainability of their business(Parulian et al., n.d.).

3. Financial losses

Phishing attacks also result in financial losses to the company which can include loss of company money, loss of important items and security costs from corporate phishing attacks, as these phishing attacks often lead to the theft of financial information, such as credit card numbers and banking passwords. The impact can be financially devastating for the victim.

4. Psychological impact

Phishing attacks have the potential to seriously damage a person's emotional state, including symptoms of depression, anxiety, anger, helplessness, embarrassment, and difficulty sleeping. In addition to the psychological attack caused by others blaming them for being a phishing victim, victims of identity theft may suffer even more from being unable to create a new identity(Pringsewu & Septasari, n.d.).

Prevention of Phishing Attacks

With the increasing use of digital technology and the internet, phishing attacks have become one of the biggest threats in cyberspace. Phishing attacks are also growing and increasing over time. The figure below shows the increasing trend of phishing attacks globally from 2021 to 2023, highlighting the increasing number of reported attacks based on data from the Anti-Phishing Working Group (APWG). It can be seen that the number of phishing attacks increased significantly from around 200,000 in early 2021 to peak in 2023 at almost 700,000 attacks, although there were fluctuations in some periods(Phishing E-Mail Reports and Phishing Site Trend.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

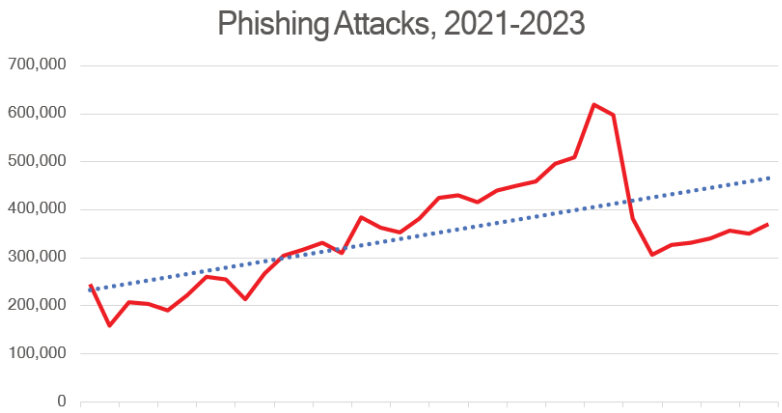

Figure 2. Number of Phishing Attacks Between 2021-2023

Phishing attacks not only occur globally but also have a significant impact in Indonesia. Based on the Indonesia Anti-Phishing Data Exchange (IDADX), phishing reports during 2023 have varied in number where the highest phishing report occurred in February 2023 with 15,050 and the lowest phishing report occurred in November 2023 with 1,729. reports occurred in November 2023 with 1,729. The following graph illustrates the number of phishing attacks reported during the period(Laporan Aktivitas Phishing Domain ~.Id Indonesia Anti-Phishing Data Exchange, n.d.).

Figure 3. Number of Phishing reports during 2023

Based on this data on the number of phishing attacks worldwide and in Indonesia, it is important to understand how these attacks can be prevented and mitigated to protect individuals and organisations from adverse impacts. The next section will discuss strategies and steps that can be taken to prevent phishing attacks and mitigate the associated risks(Süzen, 2023). The following is an analysis of some phishing attack prevention methods that can be used by individuals and organisations:

1. User Education and Awareness

Education is one of the most important steps in phishing prevention. Users need to be trained to recognise the signs of phishing and understand the risks involved. Periodic training programmes and phishing simulations can help raise user awareness. This education can improve users' awareness and ability to recognise phishing attacks. However, this education requires significant time and resources for effective and continuous training(Prasetyo et al., 2019).

2. Installing Antivirus Software

Installing antivirus software is an important step to be protected from phishing attacks and various security threats, including malware, viruses and other cyber attacks. there are several good antivirus software such as, Avast, ESET, Avira or AVG which all have free versions.

3. Enable 2-Step Verification (2FA)

Two-step verification, also known as two-factor authentication (2FA), is an additional layer of security that requires a two-time authentication process used to ensure that the person trying to access an online account is actually the owner of the account. On all your accounts, a 2-step verification process is required to be safe and avoid phishing

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

attacks. So by enabling two-step verification, you are adding an extra layer of security to your account, making it harder for unauthorised parties to access it(Indah et al., 2022).

4. Multi Factor Authentication (MFA)

MFA works by adding a layer of security by requiring users to provide more than one form of identity verification before accessing an account. This can be a combination of a password and a code sent to the user's mobile phone. MFA can add an extra layer of security that is very effective in preventing unauthorised access. However, MFA can also be inconvenient for users and may not be implemented consistently across an organisation. With users implementing this method, it can also avoid irresponsible phishing attacks.

5. Encryption and Data Security

Use encryption to protect personal data so that even if the data is stolen, the information cannot be used without the right decryption key. Also, implementing strict data security policies to restrict access to sensitive information. These techniques can protect data even in the event of a breach and also, require effective key management and can slow down access to data(Hafid et al., n.d.).

6. Plugin Browser Anti Phishing

To increase your security every time you visit a website, you can also install plugins. These tools will ascertain if there are any documents or evidence of blacklisted websites. Stop Phishing, Netcraft Extension, and Anti-Phishing and Authenticity Checker are some of the top anti-phishing plugins.

7. Use Software Firewall

Firewalls serve as the first line of defence in protecting networks and computers from cyberattacks, including phishing attacks. Although a firewall is not a specialised tool for dealing with phishing, it plays an important role in the prevention of these attacks. if there is incoming traffic, it will be checked by this software and will check the source and find out, whether it is included in the blocklist or not.

8. Using SSL Certificate

SSL (Secure Socket Layer) certificates provide an additional layer of security by encrypting the data transmitted between the user and the server, making it difficult for third parties to access the information. The use of SSL can also help ensure that users are accessing a legitimate website, as browsers will display a security mark (such as a padlock icon) if the site uses a valid SSL certificate. In addition, SSL certificates give users more confidence, increasing the reputation and credibility of the website(Muchtar et al., n.d.).

9. Check Received Emails And Messages

When you receive an email, always consider the information and intent of the sender. To determine if an email is from a legitimate domain, look at the email header, make sure the sender of the chat or SMS you received is an official account (usually marked with a check mark), and that they use a platform name, not just a phone number.

10. Filters Email and Scanning

It uses advanced email filters and scanning to detect and block phishing emails before they reach the user's inbox. These technologies often use machine learning and behavioural analysis to identify threats. This can prevent most phishing emails from being sent to users. However, it's not perfect and some sophisticated phishing emails may still slip through(Prasetia et al., n.d.).

There are also several steps that can be taken when you have already clicked on a phishing link, namely by turning off cellular data or WiFi, this is the first step if you are trapped by phishing, then delete internet browser history, this can clean up traces when we are online on the internet, then clean the device storage cache, then you can change your password, changing your password will secure your account, then next Collect evidence of phishing attacks, this can help us when we want to report phishing actions, then after collecting it, you can report phishing actions to the authorities(Ayunda, 2021).

With increased knowledge and awareness, individuals and organisations can more effectively protect themselves from phishing attacks. Continued awareness and education about this cybercrime is key to reducing the risk of falling victim to phishing, as well as ensuring the security of personal data and other important information. Reporting phishing incidents to the authorities can also help enforce the law and protect the public from this cybercrime threat(Mufti Prasetyo et al., n.d.).

CONCLUSION

Phishing has evolved from simple email scams in the 1990s to sophisticated, multi-vector attacks using AI and social media today. Modern phishing techniques include spear phishing, whaling, vishing, smishing, and deepfake AI, which target specific individuals or high-level executives. The impact of phishing ranges from personal data loss and financial harm to reputational damage and psychological distress. Effective prevention strategies include user education, antivirus software, multi-factor authentication, SSL certificates, email filtering, and reporting incidents to authorities. These measures help individuals and organizations protect themselves from the growing threat of phishing attacks.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

REFERENCES

Aptika dan IKP, P., Litbang SDM, B., & Jl Medan Merdeka Barat No, K. (n.d.). *TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX Maulia Jayantina Islami TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View Maulia Jayantina Islami*.

Ardiyanti, H. (n.d.). *CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA*. http://kominfo.go.id/index.php/content/detail/3980/

Ariadi, F., Saputra, S., & Putri, A. T. (2023). *JARI: Jurnal Pengabdian Kepada Masyarakat Republik Indonesia SOSIALISASI ANCAMAN DAN PENCEGAHAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA KEPADA SISWA/I SMK RICARDO AUTO MACHINE*. *1*(2). https://mypublikasi.com/index.php/JARI

Ayunda, R. (2021). *Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia*. https://ejournal.undiksha.ac.id/index.php/jkh

Candiwan, C. (2016). *ANALYZE PHISING THREATS IN ONLINE BANKING SERVICES*. https://www.researchgate.net/publication/303216105

Danuri, M. (n.d.). *TREND CYBER CRIME DAN TEKNOLOGI INFORMASI DI INDONESIA*.

Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, P. S., Hukum, I., Wijaya, U., & Surabaya, K. (n.d.). *Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara*.

Indah, F., Sidabutar, A., Annisa, N., Grafis, D., Multimedia, K., Negeri, P., & Kreatif, M. (2022). *Jurnal Bidang Penelitian Informatika Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)* (Vol. 1, Issue 1). https://ejournal.kreatifcemerlang.id/index.php/jbpi

Kurniawan, A. (2024). ANCAMAN DAN PENCEGAHAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA KEPADA SISWA SISWI SMK PUSPITA BANGSA. In *Praxis: Jurnal Pengabdian Kepada Masyarakat* (Vol. 4, Issue 1). http://pijarpemikiran.com/

LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID Indonesia Anti-Phishing Data Exchange. (n.d.). http://www.apwg.org,

Muchtar, P., Bintang Al -Faridzi, M., Rafli Rismawan, M., & Ul Hosnah, A. (n.d.). *MENJELAJAHI DUNIA CYBER TANTANGAN, PELUANG, DAN ETIKA DI ERA DIGITAL*. http://jurnal.kolibi.org/index.php/kultura

Mufti Prasetyo, S., Lemur, J., Firmansyah, A., Putri, A., Desi Udut, D., Maulana, D., Dian Margareta, L., Muhammad Syafiq, Y., Dwi Putra, W., & Bachtiar, N. (n.d.). *Sosialisasi Internet Sehat Pada Sosial Media Dan Waspada Terhadap Pishing Di SMPN 23 Tangerang Selatan*. https://jurnalmahasiswa.com/index.php/appa

Nugroho[1], H., Ihsan[2], M. N., Haryoko[3], A., Màarif, F., Alifah, F., & Binaniaga Indonesia, U. (n.d.). *Alahyan Jurnal Pengabdian Masyarakat Multidisiplin (ECOS-PRENEURS) Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising*.

Nur'adila, R. (n.d.). *Tren Keamanan Menggunakan Artificial Intelligence*.

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (n.d.). *Ancaman dan Solusi Serangan Siber di Indonesia*. http://ejournal.upi.edu/index.php/TELNECT/

Phishing E-mail Reports and Phishing Site Trends 4 Brand-Domain Pairs Measurement 5 Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks 6 Use of Domain Names for Phishing 7-9 Phishing and Identity Theft in Brazil 10-11 Most Targeted Industry Sectors 12 APWG Phishing Trends Report Contributors 13 4 th Quarter 2023 PHISHING ACTIVITY TRENDS REPORT. (2024). www.apwg.org,

Prasetia, O., Machfud, S., Ibnurhus, G. A., & Kunci, K. (n.d.). *SOSIALIASI PENGENALAN PENTINGNYA CYBER SECURITY GUNA MENJAGA KEAMANAN DATA DI ERA DIGITAL PADA SISWA/I SMK BAKTI IDHATA JAKARTA 1**. https://jurnal.astinamandiri.com/index.php/JIPM

Prasetyo, F., Putra, E., Irwanto, T. J., & Heryadi, A. Y. (2019). The Design and Implementation of Management Information System on Student Real Work (Kkn) in Madura University. *International Journal of Civil Engineering and Technology*, *10*(2), 159–175. http://www.iaeme.com/IJCIET/index.asp159http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=10&IType=02http://www.iaeme.com/IJCIET/index.asp160http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=10&IType=02

Pringsewu, U. A., & Septasari, D. (n.d.). *Aisyah Journal of Informatics and Electrical Engineering Cyber Security and The Challenge of Society 5.0 Era in Indonesia*. http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Radiansyah, I., & Priyadi, Y. (2016). ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING. *Bulan Januari Tahun*, *7*(1), 1–14. http://ejournal.umm.ac.id/index.php/

Süzen, A. A. (2023). Examining Social Engineering Attack Vector in Line of Data Breach. *Temmuz 2023 Journal of Technical Science*, *13*(2), 50–56. https://doi.org/10.35354/tbed.1310185

Wijoyo, A., Saputra, A., Rio Arya Pratama, M., & Rahman, R. (n.d.). *Analisis Serangan Phising dan Strategi*

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.4357

Deteksinya. https://journal.mediapublikasi.id/index.php/jriin

Yani, M. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61–78. www.ssoar.info78.https://