# Preliminary Review of Phishing Attacks and Countermeasures on the Internet of Things (IoT) Environment

Nor Naematul Saadah Ismail
School of Computing, College of Arts and Sciences
Universiti Utara Malaysia
Sintok, Kedah, Malaysia

Mohamad Fadli Zolkipli
School of Computing, College of Arts and Sciences
Universiti Utara Malaysia
Sintok, Kedah, Malaysia

## ABSTRACT
Cybercriminals now have a perfect target thanks to the growing popularity of the Internet of Things (IoT), which has increased the number of gadgets connected to the internet. In conjunction with the usage of Internet Protocol version 6 (IPv6), every device can get connected to the Internet. With this tremendous usage of devices along with Internet connection, one of the most prevalent forms of cyberattacks that target IoT devices is the phishing attack, which aims to gain owner's privileges and can make data loss. This study offers a basic analysis of phishing attacks and defenses in the context of the Internet of Things. It discusses the fundamental ideas behind phishing assaults, their types, and characteristics, as well as the most recent trends and methods that cybercriminals are using to carry out these attacks. It also examines the current countermeasures for phishing attacks on IoT devices. This paper summarizes the present state of knowledge regarding phishing attacks in the IoT environment and emphasizes the need for establishing strong defenses against these attacks for IoT devices.

## Keywords
Internet of Things (IoT), Phishing Attack

## 1. INTRODUCTION
The rapid growth of technologies and numbers of Internet users nowadays as well as advances in wireless protocols, software systems, and IPv6 standardization over the last few years point to a future in which every physical object that can benefit from an Internet connection will be connected to the Internet[1]. According to [2], without the need for human intervention, these devices are linked to the internet. Because of the internet of things' weak configuration and unique characteristics, it has become a strong target for cyber-attacks, which concerns the general user of these devices. Besides, IoT vulnerabilities are increasing daily, and they are vulnerable to a variety of attacks. Traditional security measures for IoT devices and vulnerabilities, such as authentication, access control, network security, and encryption, are insufficient, ineffective, and incapable of dealing with these problems. Meanwhile the word "phishing" can said as similar with "fishing" where fishing is to catch the fish while the "phishing" is to fish for victims' login credentials for identity theft [4]. According to researchers in [3], they stated that the Internet of Thing's (IoT) architecture has four layers which are perception, network, processing, and application. Figure 1 below shows the example of services that reside on each layer which are the first layer is application, second layer is processing layer, while the third layer is network layer and lastly the perception layer.

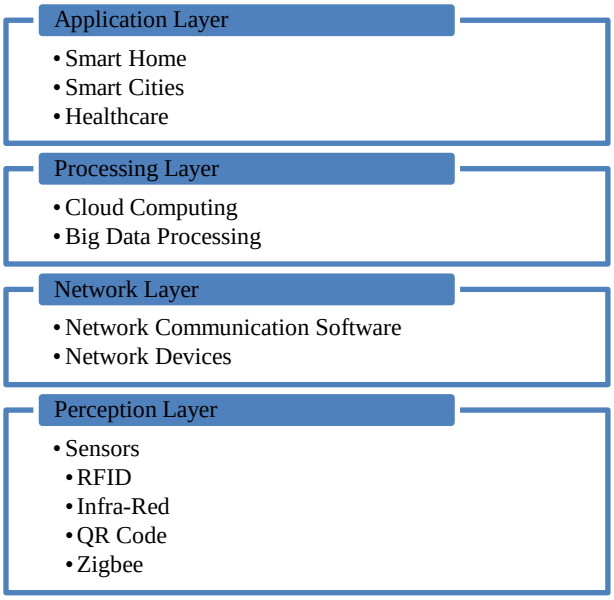



**Figure 1: Example of services at each of the IoT layers**

This study will be organized as follows. Section 2 will briefly explain the theory behind phishing attacks, the Internet of Things (IoT), and phishing in IoT. While Section 3 will cover the existing method to detect phishing in IoT and lastly Section 4 will discuss the countermeasures of phishing in the IoT environment.

## 2. LITERATURE REVIEW
### 2.1 Phishing Attack
Phishing is one of the cybersecurity threats that existed for over twenty years. It also can be defined as a criminal element that fully utilizes social engineering skills combined with a technical effort to steal for person's private information usually related to financial account details [5]. According to [6] financial institutions are at 23.6% of global phishing attacks during the first quarter of 2022. Furthermore, web-based software services and webmail accounted for 20.5 percent of attacks, making these two industries the most targeted for phishing during the examined quarter. The graphical representation of targeted type industries for phishing attacks can be referred to the Figure 2 below.

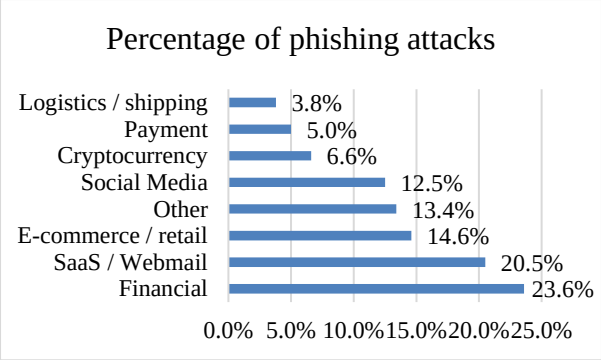



**Figure 2: Type of industries attacked by phishing.**

From the Figure 2 above, it can be concluded as financial sectors became the most targeted sector for attacker to perform phishing attack.

### *2.1.1 Phishing attack life cycle*

Researchers in [7] mentioned that there are five phishing attack life cycles which are planning and setup, phishing, infiltration, data collection, and exfiltration. The details of each cycle have been summarized in Table 1 below.

**Table 1: Five phishing attacks life cycles**

| Cycle | Description |
|---|---|
| Planning and setup | Target has been spotted and started the information gathering. |
| Phishing | Create a malicious link that will lure the victim to provide confidential information |
| Infiltration | Drive the victim to the malicious website |
| Data Collection | Financial loss possibly happens if the user discloses her private details. |
| Exfiltration | The attacker will remove the traces after getting the desired information. |

### *2.1.2 Types of phishing Attacks*

There are ten types of phishing attack as mentioned in [7] that has been summarized in Table 2 below.

**Table 2: Types of phishing attacks**

| Types of phishing attacks | Action performed |
|---|---|
| Deceptive | Personal credentials are depicted and used by the attacker as he likes. |
| Clone | The original link has been embedded in malicious form so that access can be obtained and information can be extracted. |
| Man in the middle | Phisher eavesdropped and ambush the message during transmission. |
| Evil twin | WiFi exploitation by changing the network name and snoop the network traffic. |
| Hyper Text Transfer Protocol (HTTP) | Link to a malicious website being shared by deploying the website defacement. |
| Smshing | Sending the malicious link via short message service(sms) |
| Spear | Social engineering attack to lure victim disclosing her personal credentials. |
| Vishing | Make a phone call and persuade victim to trust them. |
| Whaling | The perpetrator aims to rob the victim of their powerful and affluent status. |
| Domain spoofing | Change the legal website domain to illegal and create website defacement. |

## 2.2 Internet of Things

The fundamental idea behind IoT is to alter daily life by making smart, innovative machines and devices lawful everywhere to carry out ordinary tasks with the least amount of human interaction. Even though it may seem difficult to attain, it is a truth that many aspects of the Internet of Things will be revealed in the not-too-distant future. IoT is used for entertainment purposes as well, such as in TV shows, news, cartoons, and movies. [8]. A group of physical objects embedded with electronics, circuits, application software, sensors, and network connectivity made up the Internet of Things (IoT). This group can collect and exchange data among themselves through the Internet connection [9]. This technology makes us rely upon the Internet in our daily life. IoT has grown rapidly making so much revolution in almost every sector. Because of Internet technologies, security threats towards IoT devices became disruptive [10]. As shown in Figure 3 below, there are lots of IoT applications in various fields.

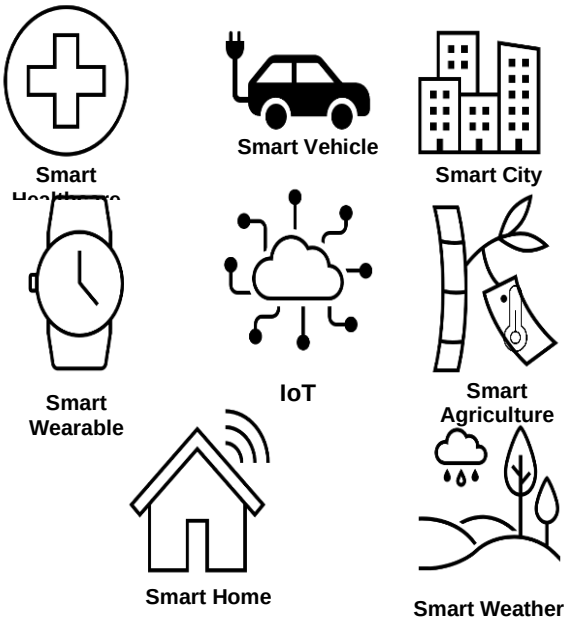



**Figure 3: IoT applications in various fields**

## 2.3 Phishing in IoT

In recent years, the insufficient security measures in place have resulted in numerous attacks on IoT devices. As the number of available IoT devices grows, these attacks are also increasing. This can be attributed to manufacturers prioritizing the production of IoT devices and neglecting security measures, driven by high consumer demand and intense vendor

competition. Given the widespread use of IoT devices across various sectors including organizations, industries, and government agencies, there is a significant risk of catastrophic effects resulting from IoT device exploitation and data breaches. Hackers are exploiting the vulnerabilities of IoT devices to gain control and engage in malicious activities, such as botnet attacks and exposure of valuable and confidential information, ultimately leading to financial loss [10]. Phishing mainly targeted on systems of financial and banking sectors, usually intended for money purposes [11].

Phishing in the IoT environment can have a significant impact on not just organizations, but also individuals and governments. There are a few phishing cases involving IoT quite recently. According to Gartner, businesses have lost millions of dollars as a result of phishing attempts on different hosting devices and when utilizing their apps [12]. Another phishing attack history in IoT has been simplified in Table 3 below.

**Table 3: IoT attack in history**

| Sector/case | Consequences |
|---|---|
| Banking domain (2018) | Money has been tapped online or through an auto teller machine (atm) |
| Google Play Store (2018) | mAadhaar application database has been breached causing the users' information disclosure |
| eGadget+ (December 2016) | Involved in the delivery of more than 750,000 malicious emails to hundreds of thousands of devices, including handheld and networking devices such as routers |
| Fifty Russia big companies (Nov 2018 – Feb 2019) | Hackers sent a massive email attack containing encrypted virus Shade/Troldesh, asked for mo |
| (Dec2016) | More than 750,000 malicious emails were sent to various types of devices as reported by egadget+ in India. |

# 3. EXISTING RESEARCH ON THE DETECTION OF PHISHING ATTACK

## 3.1 Machine learning mechanism

Network forensics is one of the areas in digital forensics and is being built by fully utilizing machine learning methods. It monitors and inspects the network traffic. Three techniques have been classified by [12], which are logistic regression (LR), random forest (RF), and support vector machine (SVM). The experiment was done by performing data collection. UNSW-NB15 is the dataset that has been used and designed by the Australian Center of Cybersecurity. The goal for this experiment was to monitor and inspect network traffic to determine the accuracy, sensitivity (TPR), specificity (TNR), precision, F-measure and false alarm rate for each techniques. The result from the experiment can be referred to in Table 4 below and can be explained as random forest had the highest accuracy (96.85%), followed closely by support vector machine (96.74%), while logistic regression had the lowest accuracy (92.29%). In terms of sensitivity (true positive rate), random forest also had the highest score (98.41%), followed by support vector machine (97.85%), and then logistic regression (93.02%). The true negative rate (specificity) was highest for support vector machine (95.87%), followed by random forest (95.65%), and then logistic regression (91.73%).

In terms of precision, random forest had the highest score (94.55%), followed closely by support vector machine (94.87%), and then logistic regression (89.67%). The F-measure, which is the harmonic mean of precision and sensitivity, was highest for random forest (96.44%), followed by support vector machine (96.33%), and then logistic regression (91.31%). Finally, the false alarm rate was lowest for random forest (3.14%), followed by support vector machine (3.25%), and then logistic regression (7.71%). As the conclusion the results suggest that random forest and support vector machine are both effective techniques for network forensics using the UNSW-NB15 dataset, while logistic regression is less accurate.

**Table 4 : Performance of different Algorithm**

| | RF | SVM | LR |
|---|---|---|---|
| Accuracy | 96.85% | 96.74% | 92.29% |
| TPR | 98.41% | 97.85% | 93.02% |
| TNR | 95.65% | 95.87% | 91.73% |
| Precision | 94.55% | 94.87% | 89.67% |
| F-Measure | 96.44% | 96.33% | 91.31% |
| False Alarm Rate | 3.14% | 3.25% | 7.71% |

## 3.2 Lightweight Data Representation

Researchers in [13] have proposed an approach for detecting phishing websites in an Internet of Things (IoT) environment. The approach involves using a lightweight data representation and applying feature selection methods, specifically Information Gain, Chi-Squared, and Relief, to rank and select the most relevant features for detecting phishing websites. The researchers suggest that their approach could be used as a starting point for developing cybersecurity solutions for IoT devices, which are becoming increasingly vulnerable to attacks as they become more prevalent and interconnected.

## 3.3 Anti-Phishing

Researchers in [14] mentioned that anti-phishing method was under defense model that has been categories for protection and multilevel defense. Thus, the technique has been summarized as non-technical methods, which includes legal measures and education. Legal measures aim to provide the proper legal recourse against phishing attacks, although it is not effective against more serious threats. Education, on the other hand, helps individuals to identify phishing emails through training and simulated phishing emails. The second category is technical anti-phishing techniques. Black- and whitelisting is the primary method to mitigate the threat of phishing websites. Blacklisting maintains an extensive list of suspicious or harmful sites, while whitelisting is a database of legitimate sites. However, whitelisting is impractical as it is difficult to predict the sites users will go to, and new sites would be classified as suspicious even if they are legitimate. Heuristic detection involves extracting features from phishing sites, while visual similarity detection computes the similarity between suspicious sites and a database of legitimate website features. Machine learning techniques have also been implemented, such as decision trees, neural networks, and support vector machines (SVM), which focus on classifying phishing emails, messages, and websites.

# 4. COUNTERMEASURES OF PHISHING ATTACK IN IOT NETWORK

Authors in [15] classified various phishing detection and protection against phishing which are email filtering and phishing website detection. But before that, user education will come first as the phishing attacks motivation is to lure victim to provide confidential information. Besides that, authors [16] classified phishing attacks into human based and technology based. To educate users regarding the awareness can take the

education industry as well as the government agencies to made efforts by delivering the education to the youngsters and could enable public citizen understand more about cybersecurity [15].

### 4.1 Educate Users

When our personal information being disclosed to the cybercriminals, they can convert our good reputation into bad one and make the identity theft successes. Thus researchers in [7] provided the suggestion that has been simplified as in Table 5 below.

**Table 5 : Phishing attacks prevention suggestion**

| Suggestion | Description |
|---|---|
| Keep informed about phishing techniques | Users need to keep up to date with current threat |
| Think before you click | Do not click on random link received. Mouse over link to see the actual unified resource locater (URL) |
| Install anti-phishing toolbar | Customize browser with security features |
| Keep browser up to date | Update web browser accordingly |
| Use firewalls | Enable firewall inside router or in small network |
| Verify site's security | Make sure there is secure hypertext transfer protocol (https) when using website or application that disclosing personal information |
| Online account frequently checks | Change password regularly |
| Worry about pop up | Do not react to any popup windows. Click small "x" preferably. |
| Never share personal information | Remain cautious when involving personal information disclosure |
| Use antivirus software | Install antivirus on both mobile and laptop/desktop |

As we believe that phishing usually related with human action and behavior, it is important to educate users and raise their awareness of phishing techniques and risks. By adopting safe online practices such as verifying the legitimacy of links, not sharing personal information, and updating their security measures, users can significantly reduce the likelihood of falling victim to a phishing attack. Additionally, it is essential to establish a culture of cybersecurity both in organizations and among individuals, where cybersecurity is seen as a shared responsibility and a priority for everyone. Ultimately, human action and behavior can be the first line of defense against phishing attacks, and the importance of educating and raising awareness cannot be overstated.

### 4.2 IoT Cyber Threat and Countermeasure Overview

Researchers in [17] have classified various cyber threats that happened together with their countermeasures. Attacker pretended to become a trusted entity by masquerading the legitimate user. This action caused the IIoT system breached. Thus, the countermeasures that has been identified are as follows:

- Phishing attacks auto detection and analysis using PHONEY
- Using Intelligence Web Application Firewall
- Embedding the URL
- Mapping a sequence model based by extracting URLs from malicious emails to detect botnets.
- Implement zone-based firewall policy to detect malicious domain names that has been generated algorithmically .

### 4.3 Securing IoT in Smart Home Platforms

Smart home platform is one of the application in IoT. [18] have summarized the methods to thwart the IoT attack as explained below:

- Jamming attack: change the frequency of communication channel.
- Traffic analysis attack: implement traffic encryption on the network.
- App Over privilege: use code analysis and natural language programming.
- Unauthorized device: add authentication to application and authentication among IoT devices.
- Voice spoofing attack: distinguish the voice sample so that attacker cannot imitate the original voice.

Therefore, securing IoT devices in smart home is critical to protect against various type of cyber threats, especially phishing attack. As the use of smart home devices continues to increase, it is important to implement these countermeasures to safeguard against potential cyber threats.

## 5. CONCLUSIONS

In conclusion, as the popularity of IoT devices grows, they become a more attractive target for cybercriminals, and phishing attacks are one of the most common methods used to compromise them. This paper has provided an overview of the types, characteristics, and techniques of phishing attacks in the context of IoT, as well as the countermeasures available to protect against them. User education and awareness are critical to reducing the success of phishing attacks, as human actions and behaviors play a significant role in preventing such attacks. However, technology-based defenses such as anti-phishing toolbars, web application firewalls, and advanced machine learning algorithms are also crucial to mitigating the risks posed by phishing attacks. It is essential for IoT device users to remain vigilant and take proactive measures to protect their devices and personal data from online threats. As the IoT landscape continues to evolve, it is crucial that individuals and organizations remain informed and adaptable in their approach to cybersecurity.

For future works on this topic, we suggest for investigating the effectiveness of existing prevention methods. Besides that, human factor can be focused on to determine the human behavior toward phishing attack so that it can be mitigated. Other than that, the impact of IoT device design and the usage of artificial intelligence can be focused on.

## 6. ACKNOWLEDGMENTS

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

## 7. REFERENCES

[1] A. Dunkels *et al.*, "Low-power IPv6 for the internet of

things," *9th Int. Conf. Networked Sens. Syst. INSS 2012 - Conf. Proc.*, 2012.

[2] S. A. Haifa Ali and J. Vakula Rani, "Attack Detection in IoT Using Machine Learning—A Survey BT - Intelligent Cyber Physical Systems and Internet of Things," 2023, pp. 211–228.

[3] T. Aziz and E. Haq, "Security Challenges Facing IoT Layers and its Protective Measures," *Int. J. Comput. Appl.*, vol. 179, no. 27, pp. 31–35, 2018.

[4] H. Thakur and S. Kaur, "A Survey Paper On **Phishing** Detection," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 4, pp. 64–69, 2016.

[5] K. Nirmal, B. Janet, and R. Kumar, "Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2327–2339, 2021.

[6] Ani Petrosyan, "Online industries most targeted by phishing attacks," 2022. [Online]. Available: https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/.

[7] A. Sadiq *et al.*, "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 5, pp. 854–864, Dec. 2021.

[8] S. Gautam, A. Malik, N. Singh, and S. Kumar, "Recent Advances and Countermeasures against Various Attacks in IoT Environment," *2nd Int. Conf. Signal Process. Commun. ICSPC 2019 - Proc.*, pp. 315–319, 2019.

[9] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to IoT," *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 5, no. 1, pp. 41–44, 2018.

[10] S. G. Abbas *et al.*, "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach," *Sensors*, vol. 21, no. 14, pp. 1–25, 2021.

[11] K. Nirmal, B. Janet, and R. Kumar, "Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2327–2339, 2021.

[12] S. Naaz, "Detection of phishing in internet of things using machine learning approach," *Int. J. Digit. Crime Forensics*, vol. 13, no. 2, pp. 1–15, 2021.

[13]L. Bustio-Martínez, M. A. Álvarez-Carmona, V. Herrera-Semenets, C. Feregrino-Uribe, and R. Cumplido, "A lightweight data representation for phishing URLs detection in IoT environments," *Inf. Sci. (Ny).*, vol. 603, pp. 42–59, 2022.

[14]R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Futur. Internet*, vol. 12, no. 10, pp. 1–39, 2020.

[15]B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, pp. 1–32, 2017.

[16]H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," *Future Internet*, vol. 11, no. 3. MDPI AG, 2019.

[17]K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, 2021.

[18]Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 53–59, 2018.