# *Guarding Against Deceptive Waters:* A Literature Review of Risk Analysis and Management in Combating Phishing Attacks


**ECE 9110 001 GS23**

RISK ASSESSMENT AND MANAGEMENT

WESTERN UNIVERSITY

Kanika Gandhi *kgandh27@uwo.ca*

**Executive Summary**

This paper offers a comprehensive approach to help combat a famous cyber-attack called ‘phishing’, by performing a detailed assessment of the risks that are caused due to it. The paper initially discusses the definition, types, and method of performing the attack.

Following this, the paper analyses important risks that are associated with this attack and categorizes them into two based on the sectors they belong to. To perform a detailed risk analysis a simple technique is proposed to carefully analyse, assess, and evaluate the risks identified in both the technical and financial areas. The major takeaways are determining the criticality of the risks, which turn out to be mostly high with one moderate, understanding the cause and in-depth factors influencing it then assessing the impact of these due to their modes of exploit.

The paper highlights management techniques for each risk that can be implemented as effective strategies to first avoid, prevent, and then reduce the impact upon occurrence and finally accept the unavoidable percentage. An understudy reviews the existing solutions, that are used to detect this attack (hence prevent), in a search to identify probable research gaps.

The appendix showcases the actual basis of risk rating and the essential underlying questions to be answered during an assessment. Further it shows how phishing has taken over the cyber world followed by an evolution of detection softwares to combat this trend from previous years to date. Lastly, current detective processes have been presented to understand real time risk management.

**Introduction**

With everything digitalizing around us, the toll that cyber has taken over the world is remarkable; however, just like an ocean, this world delves deeper. But with good comes bad and similarly like many good fish in the sea, there lurk some evil ones too. Whilst silently preying on innocent individuals and organisations using wickedly crafted ways, some users carry out cyber-attacks to cause damage to reputational, financial, personal, or professional lives for personal gains and ulterior motives. One such attack, under special attention lately, is the "phishing" attack [1]. Much like its name, this attack is carried out by 'hooking' the victim using an impersonated 'bait' to deceive them into revealing any sensitive information or data [2]. As seen in Fig.1, the attack is very widespread and can be performed in five ways. From big companies to mere individuals the attack has a customization of its own to 'hook' a variety of fresh 'bait'. These attacks come with highly critical malicious risks that cause dire irreversible damage in some cases. With time, the cybercriminals, have started using sophisticated tactics and ways to 'hook' their victims via impersonation through social engineering or exploitation of vulnerabilities present in systems. Due to the rise in the occurrence of these attacks (Appendix B- B1), it is necessary to analyse and assess the risks that emerge to develop management strategies to alleviate them. By studying these escalating risks, the effect of phishing can be reduced to a great extent as it can allow implementation of secure protocols, controls, make users more aware and provide guidance in the future for building robust anti-phishing software and mechanisms.

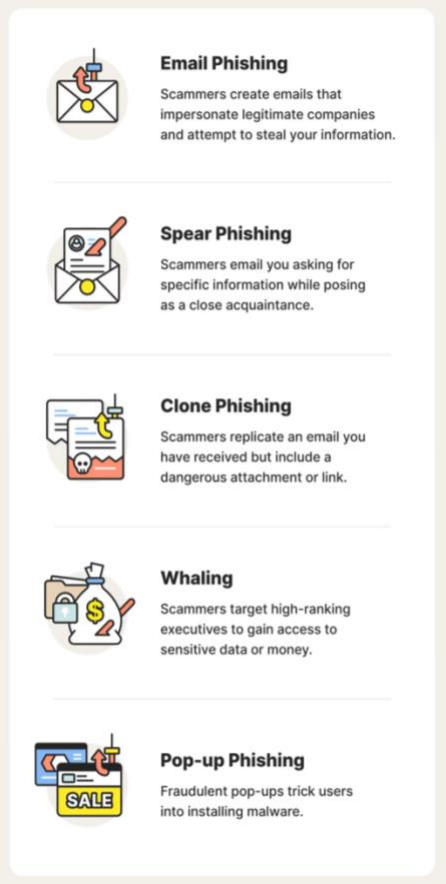


Fig.1: Types of Phishing [2]

**Risk Assessment** (Risks Associated with Phishing)

In case of phishing, there are many risks, that if materialized, can lead to the catastrophic downfall of an entire infrastructure. Risks emerge from all the sectors [3] in case of phishing and can be of financial type such as monetary loss, technical type such as compromise of sensitive information and even legal such as regulatory compliance. But the most common yet dangerous ones are:


Fig.2: Risks of Phishing (2022) [4]

1) Technical Risks
   a. Data Breach
   b. Malware Distribution
   c. Credential Harvesting
2) Financial Risks
   a. Identity Theft
   b. Financial Fraud

**Risk Assessment** (Risks Analysis)

Prior to understanding how to combat phishing attacks, it is essential to understand the cause and effect of each of the risks with their ratings (Appendix A) to completely eradicate them.

1. *Data Breach*-HIGH

   Cause: i) Presence of exploitable vulnerabilities in the software that provide back doors for access which leads to sniffing or eavesdropping attacks. ii) Lack of two-factor authentication to verify identification for user access.

Impact: Unauthorized people or personnel gain access to sensitive data and compromise the data by either stealing it, damaging it, manipulating it, or causing disruption of services [5].

2. *Malware Distribution*-MEDIUM

   Cause: i) Process of sideloading applications in mobile devices that belong to third party. ii) Lack of awareness regarding or clicking of suspicious email attachments and web-links.

   Impact: Data integrity can be highly compromised by corruption and stability of network systems can be crippled to block user access leading to long periods of server downtime [5].

3. *Credential Harvesting*-HIGH

   Cause: i) Usage of weak and easily breakable credentials or passwords. ii) Insufficient security software or inadequate web-security which leads to browser exploitation attacks.

   Impact: Malicious users can use personal credentials to perform account takeovers, perform financial transactions and invade privacy by locking users out denying them service [6].

4. *Identity Theft*-HIGH

   Cause: i) Lack of domain and sender-based email protocols for authentication. ii) Unawareness of risky vs safe surfing and lack of security training which leads to spoofing attacks.

   Impact: Unauthorized/unauthenticated users can impersonate someone else's identity to perform criminal activities and can pose a massive threat to financial and reputational loss [7].

5. *Financial Fraud*- HIGH

   Cause: i) Interaction with a compromised payment gateway or system. ii) Presence of weak transaction validation mechanisms and protocols that allow man-in-the-middle attack.

   Impact: Malicious users can use the user's vulnerability to perform heavy fraudulent transactions, access digital wallets, drain funds and damage credit score of the victim [8].

**Risk Management** (Risk Avoidance)

In risk mitigation, it is often ideal to remember that risks cannot completely be mitigated but can be handled systemically using- avoidance, loss prevention, loss reduction and lastly acceptance. So firstly, for avoidance, we can utilize the recommendations given below.

1. *Data Breach*- Firstly, implement intrusion detection systems such as Snort and apply encryption protocols on access. Secondly, introduce input sanitization to avoid injection attacks during access. Lastly, regularly perform sanitary checks and VAPT (Vulnerability Assessment and Penetration Testing) assessments to find any weaknesses and patch it [9].

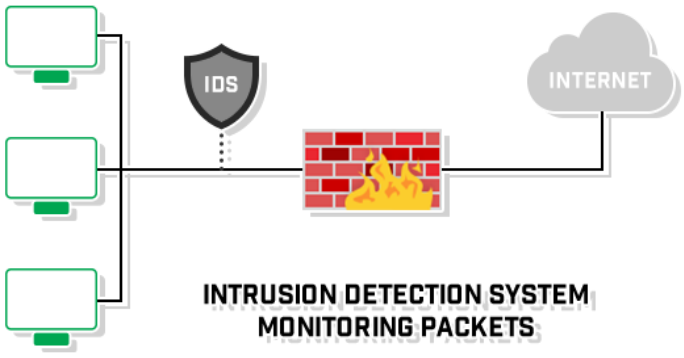


Fig.3: Intrusion Detection System [10]

2. *Malware Infection*- Firstly, implement anti-malware systems such as Malwarebytes and apply scanning mechanisms and protocols that induce threat intelligence to alert and detect any malware presence. Secondly, update all software and systems with state-of-the-art versions with bug fixtures. Lastly, spread unawareness regarding browsing safely, not clicking any suspicious links or mails [11].
3. *Credential Harvesting*- Firstly, implement stronger passwords that are encrypted and hard to break. Secondly, make sure secure transmission protocols are being used such as HTTPS instead of HTTP. Thirdly, introduce multi-factor authentication like DuoSecurity to add

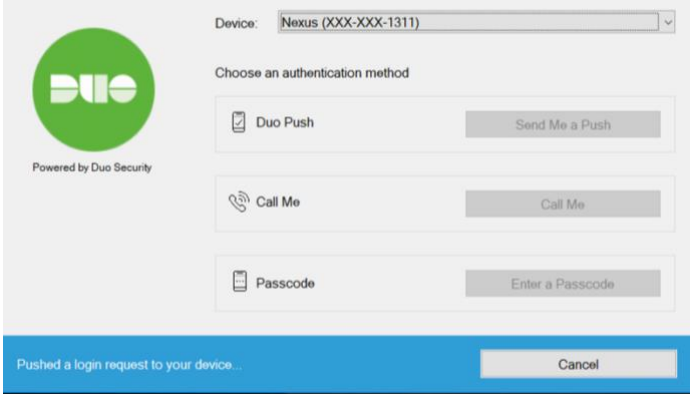


Fig.4: Duo Security Authentication [12]

layers of complication, making it harder for the attacker to gain access. Lastly, give proper security training regarding phishing to ensure vigilance [9].

4. *Identity Theft*- Firstly, implement safe client-server email interaction controls. Secondly, constantly keep an eye out for any noteworthy suspicious activity or unusual activity from the list of accounts. Lastly, utilize email authentication protocols such as SCP to verify sender info. [11].
5. *Financial Fraud*- Firstly, use encrypted and fully secure gateways to perform transactions. Secondly, utilize transaction systems to monitor and alert the user for any fraudulent activities. Lastly, deploy fraud prevention systems like IBM Trusteer and perform audits [13].

Fig.5: IBM Trusteer protected site [14]

**Risk Management** (Loss Prevention & Loss Reduction)

By covering mitigation strategies, risk avoidance is taken care of, leaving us with the next important way of risk management, that is loss prevention and reduction. With new developments, anti-phishing solutions have transformed in such a way that it is now easier to prevent loss by using anti-phishing detection software. The anti-phishing software can detect any presence of attack and alert or flag the user, preventing it from occurring at all. Post detection, these systems are also trained to use incident response plans to reduce the loss that could occur. It started off as simple classification based off blacklisting, but technology improvised their techniques to create anti-phishing solutions (Appendix B- B2). The categories are mainly- Content based and Non-Content based software [15]. Content-based includes analysing the actual content and the scanning through the main material of the site or email via either automated or rule-based approach. This can further

be broken down into machine learning based software or textual rule-based software. Although both the applications scan all detail present on a page, the former does it by learning patterns from malicious sites or mails and then applying their learned knowledge to detect anomalies in their test data. On the other hand, the latter looks for phishing indicators by comparing its test data with a set of rules that have been pre-defined to it, kind of like a checklist. However, with Microsoft Defender for Office 365 (Appendix B- B3) being the latest ML content-based software and with Sophos Email Security being the most used textual rule content-based software (Appendix B- B3), this category of anti-phishing solutions has their efficiency and limitations. The ML based solutions succeed in classifying their detection to a great degree due to availability of large sets of training data, but it fails to detect unlabelled data and hence struggles with zero-day attacks. Similarly, the textual rule-based solution exceeds expectations in providing faster results but fails to adapt with new advancements in attacks due to pre-configured set of rules and is limited to familiar attacks only, not being able to keep up with state-of-the-art techniques. Non-content based solutions, however, utilize URL & domain analysis methodologies alongside visual and image recognition. Like the name, since only a few components of the websites and malicious data are analysed, this category works more on a see-believe perspective. As Webroot Bright Cloud (Appendix B- B4) has emerged with its sharp ability to scan URLs and domains for suspicious links, it promptly gets a hold of phishing links but does have a fair amount of struggle when it comes to homograph attacks, due to the similar nature of characters present. Moreover, the recognition PhishLabs (Appendix B- B4) has received for accurate detection through visual elements is commendable as it does not fail to catch pictorially deceptive elements present on fake sites and mails (such as logos, layouts and much more). But it does too face obstacles in detecting text based phishing sites or mails that heavily rely on written information than graphics.

**Conclusion**

As organizations and people are moving more towards hosting data on cloud, shared drives, and web applications, it has become imperative to secure the information from such cyber-attacks.

Phishing attacks is one of the most common attacks nowadays [22]. The frequency of occurrence of this attack does not mean that there are no controls in place. Instead, it shows that despite there being controls they are either not implemented appropriately or have not been adopted by firms and individuals. Not attending to these attacks through periodic monitoring cannot inhibit organizations from becoming a prey to such attacks and loosing sensitive information, compromising on their reputation.

This has thrown some light on the importance of identifying potential vulnerabilities which may become problematic coming forth. Having a regular exercise (mostly annual) wherein inherent risks and current controls are identified and gaps are highlighted will help in reducing these cyber-attacks and their effects. From risk assessment and management of this attack it is evident that high level risks accompany phishing which can either be avoided through some level of generic controls and prevented through some security controls. However, the impact of risks that cannot be completely tackled can be reduced using security incident responses upon detection and those that cannot be avoided at all can have some level of safety net (business recovery plans) to bounce back from. In totality, it is not easy to avoid, but can be made easier with prior awareness through this process of risk assessment and management.

**Appendix A**

1. Procedure for risk criticality classification- Based on the definitions below, the risks are classified into three categories (Fig.A1) using the statistics of the risks as per research [16].

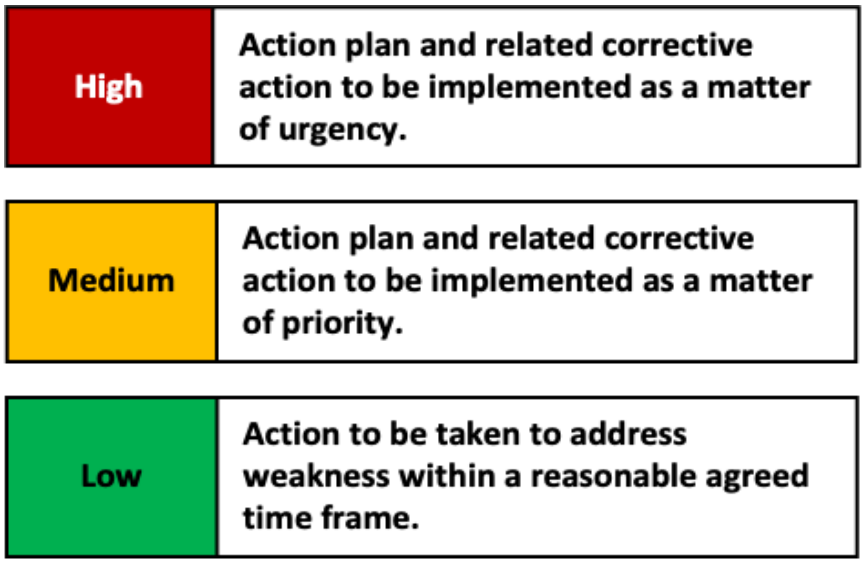


Fig. A1: Observation Rating definitions

The classification and criticality of these risks depends on the following factors:

1. How often do these risks occur?
2. How much damage do these risks pose to the organization or induvial?
3. How easily perceptive/ breach-able are these risks?
4. How much priority should be given to this risk over any other?
5. How often do these risks need mitigation plans?
6. How much time frame does the risk have to be eradicated? - i.e the shorter the time frame the riskier it is. (Also known as action time)

**Appendix B**

B1. The evolution of trend as phishing attack stands out to be the most common cyber attack in the last few years with an alarmingly high percentage of 80%.

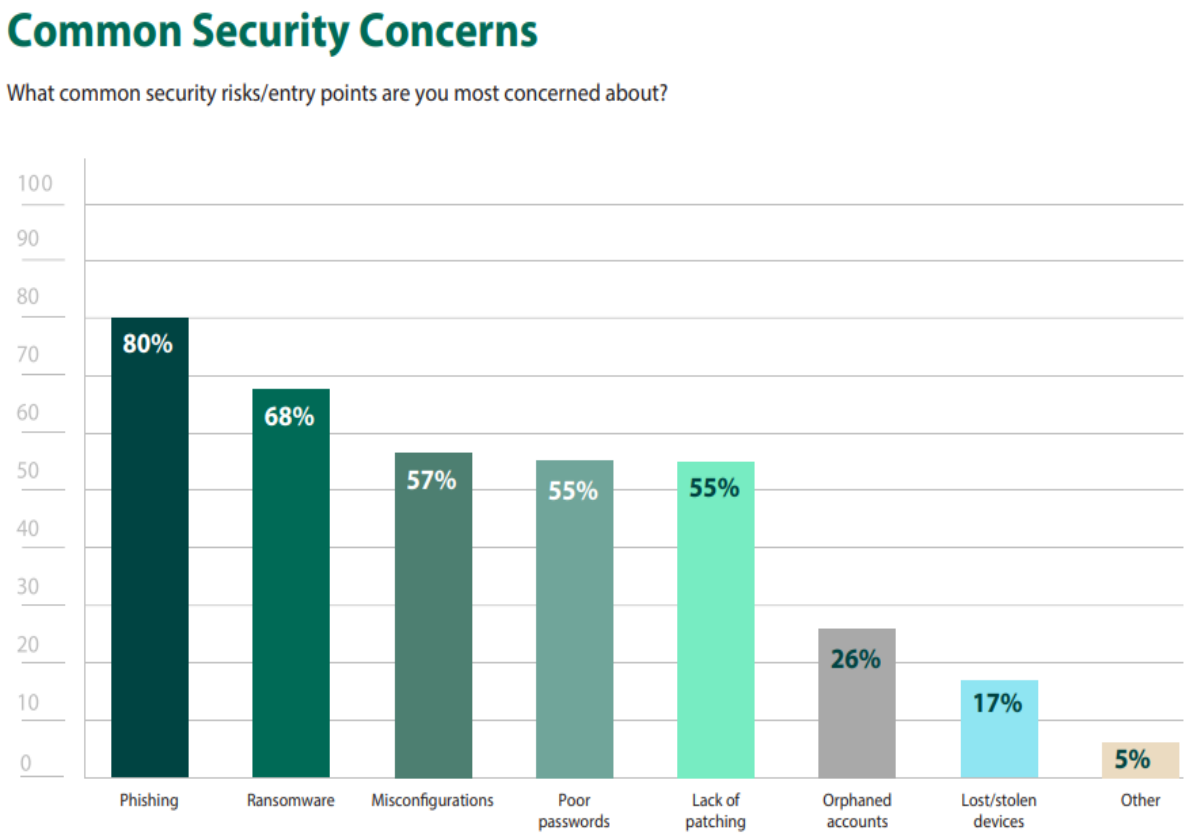


Fig. B1: Most common cyber concern distribution. [17]

Observation: Even though other attacks do compete closely with phishing they somehow fall behind due to lack of craftiness and magnitude of threat they expose comparatively.

B2. Evolution of anti-phishing softwares.

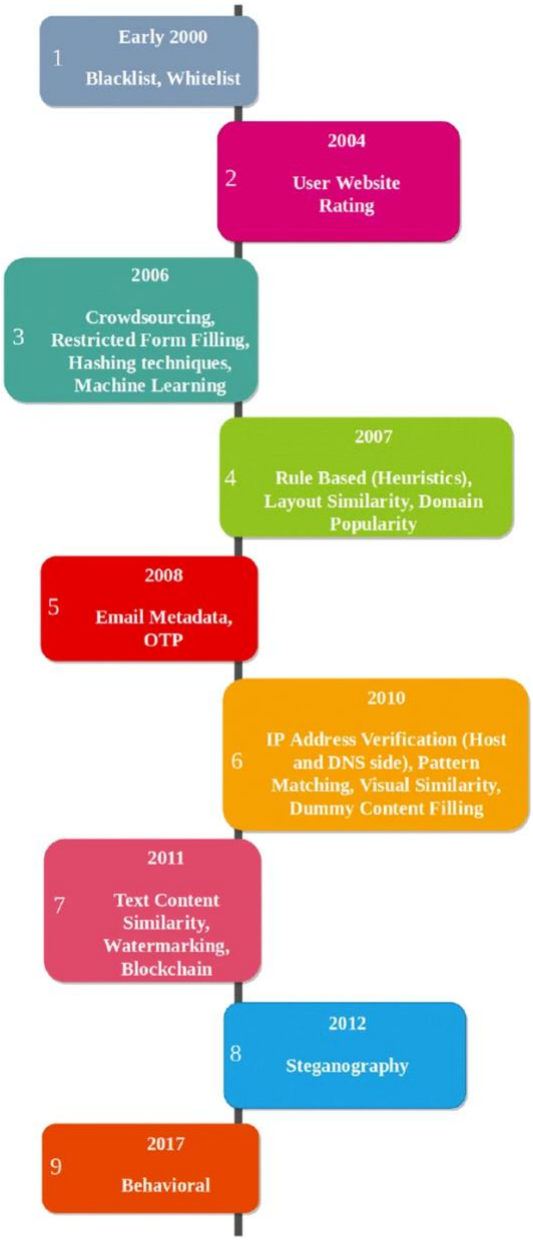


Fig. B2: Road map of evolution of anti-phishing solutions [15]

B3. Content based anti-phishing softwares.


Fig. B3-1: Threat protection approach of Microsoft Defender for Office 365 [18]

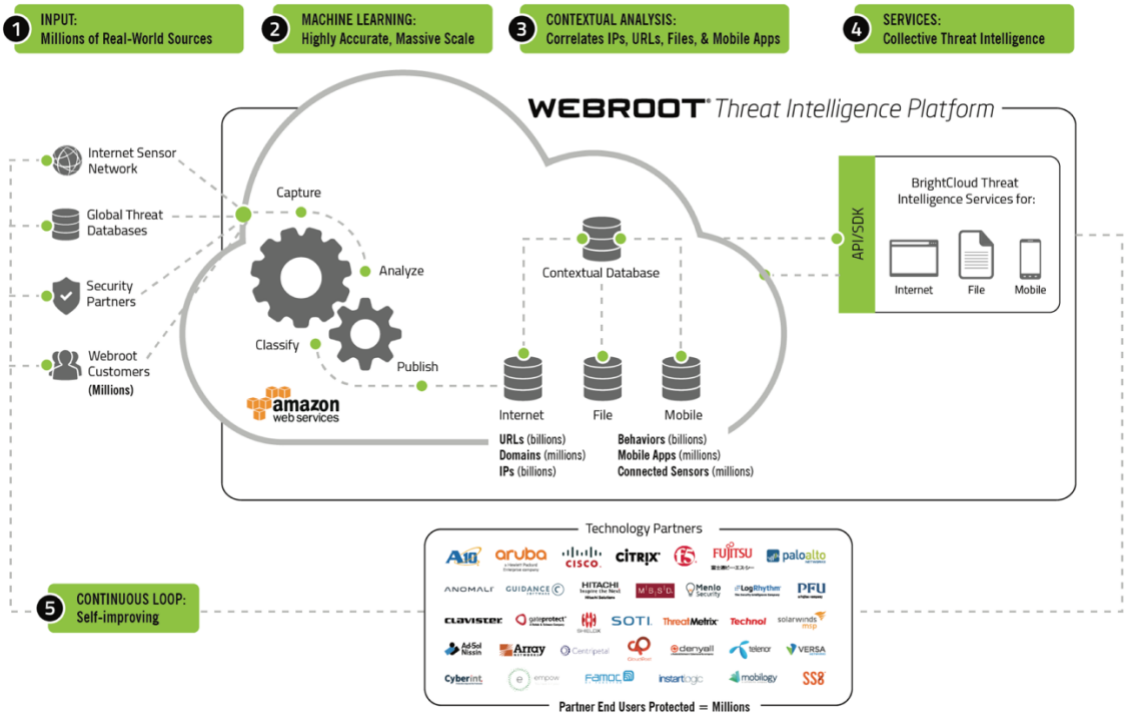


Fig. B3-2: Process of content analysis conducted by Webroot Bright Cloud [19]

B4. Non-content anti-phishing softwares.

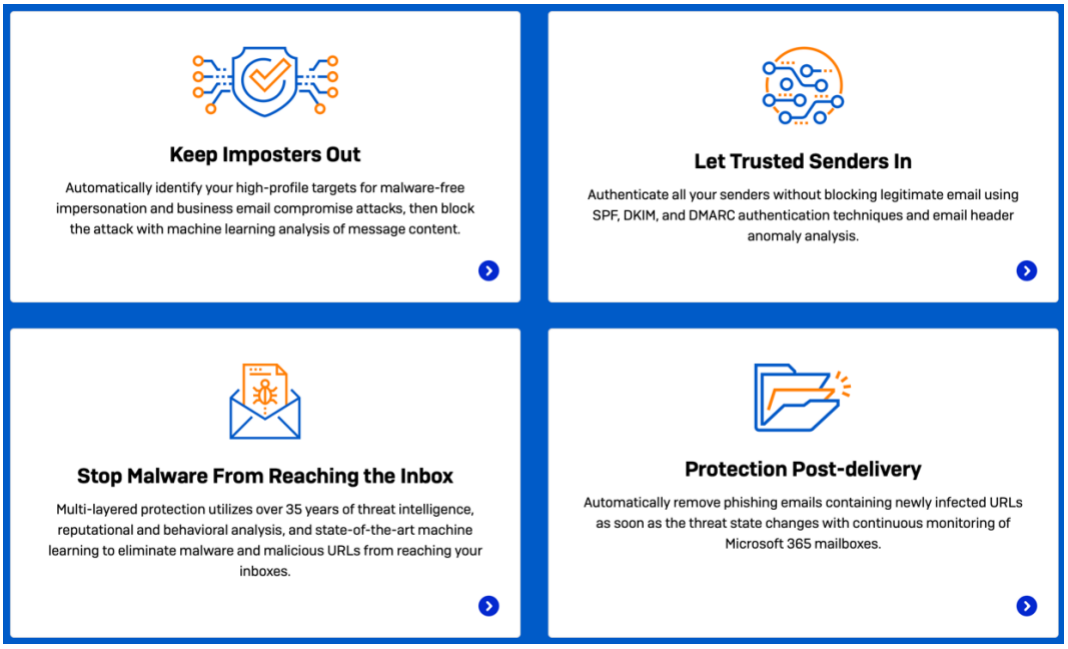


Fig. B4-1: Anti-phishing approach implemented by Sophos Email Security [20]

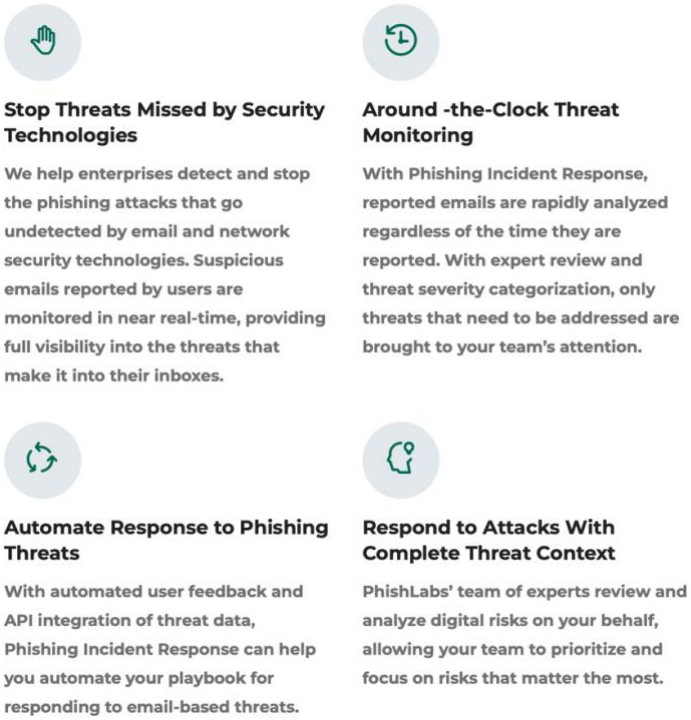


Fig. B4-2: Solutions and incident response of Phishlabs to detect and prevent phishing [21]

**References**

[1] Aleroud, Ahmed, and Lina Zhou. 2017. “Phishing Environments, Techniques, and Countermeasures: A Survey.” Computers & Security 68: 160–96. https://doi.org/10.1016/j.cose.2017.04.006.

[2] Rashid, Fahmida Y. 2020. “8 Types of Phishing Attacks and How to Identify Them.” CSO (Online).

[3] Freedman, Bradley. 2016. “Cyber Risk Management - Phishing.” Mondaq Business Briefing, 2016.

[4] Tessian, “Must-Know Phishing Statistics: Updated 2022,” Tessian, April 10, 2023, https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=Phishing%20is%20a%20huge%20threat, receiving%20an%20average%20o %2049

[5] Hadnagy, Christopher, and Michele Fincher. 2015. Phishing Dark Waters : the Offensive and Defensive Sides of Malicious e-Mails. Indianapolis, Indiana: Wiley.

[6] Bhardwaj, Akashdeep, Fadi Al-Turjman, Varun Sapra, Manoj Kumar, and Thompson Stephan. 2021. “Privacy-Aware Detection Framework to Mitigate New-Age Phishing Attacks.” Computers & Electrical Engineering 96: 107546–. https://doi.org/10.1016/j.compeleceng.2021.107546.

[7] Schwartz, Sarah. 2018. “Schools Teach ‘Cyber Hygiene’ to Combat Phishing, Identity Theft.” The Education Digest 84 (1): 4–8.

[8] Qabajeh, Issa, Fadi Thabtah, and Francisco Chiclana. 2018. “A Recent Review of Conventional Vs. Automated Cybersecurity Anti-Phishing Techniques.” Computer Science Review 29: 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003.

[9] Sadiq, Ashina, Muhammad Anwar, Rizwan A. Butt, Farhan Masud, Muhammad K. Shahzad, Shahid Naseem, and Muhammad Younas. 2021. “A Review of Phishing Attacks and Countermeasures for Internet of Things-based Smart Business Applications in Industry 4.0.” Human Behavior and Emerging Technologies 3 (5): 854–64. https://doi.org/10.1002/hbe2.301.

[10] Blog Team, “Understanding Intrusion Detection and Prevention Systems,” n.d., https://www.accessagility.com/blog/understanding-intrusion-detection-and-prevention-systems.

[11] Jampen, Daniel, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. “Don’t Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review.” Human-Centric Computing and Information Sciences 10 (1). https://doi.org/10.1186/s13673-020-00237-7.

[12] “Duo Authentication for Windows Logon - Guide to Two-Factor Authentication · Duo Security,” n.d., https://guide.duo.com/rdp.

[13] IBM to Acquire Trusteer to Help Companies Combat Financial Fraud and Advanced Security Threats: New IBM Cybersecurity Software Lab in Israel Will Focus on Mobile and Application Security, Counter-Fraud and Malware Detection. 2013. New York: PR Newswire Association LLC.

[14] Alberto Segura, “Vulnerabilidad a nivel de kernel en Trusteer Rapport para macOS,” Una Al Día, December 28, 2018, https://unaaldia.hispasec.com/2018/12/vulnerabilidad-a-nivel-de-kernel-en-trusteer-rapport-para-macos.html.

[15] Chanti, S., and T. Chithralekha. 2020. “Classification of Anti-Phishing Solutions.” SN Computer Science 1 (1). https://doi.org/10.1007/s42979-019-0011-2.

[16] Krause, Micki., and Harold F. Tipton. 2007. Information Security Management Handbook. 6th ed. Boca Raton: Auerbach Publications. https://doi.org/10.1201/9781439833032.

[17] “154 Cyber Security Statistics: 2023 Trends & Data | Terranova Security,” April 24, 2023, https://terranovasecurity.com/cyber-security-statistics/.

[18] “Microsoft Defender for Office 365 | Microsoft Security,” n.d., https://www.microsoft.com/en-ca/security/business/siem-and-xdr/microsoft-defender-office-365.

[19] Webroot, “BrightCloud Threat Intelligence Services,” n.d., https://www-cdn.webroot.com/7615/2510/6597/BC-BCTI-Overview-DS_us.pdf.

[20] Sophos, “Prevent Phishing with Sophos Email Security,” SOPHOS, March 3, 2022, https://www.sophos.com/en-us/products/sophos-email.

[21] “Phishing Incident Response - PhishLabs,” PhishLabs, n.d., https://www.phishlabs.com/phishing-incident-response/#.

[22] Farrell, Casie. 2020. “Phishing in the Financial Sector”. ProQuest Dissertations Publishing.