From January 2019 to April 2020

Phishing

ENISA Threat Landscape
Overview

Phishing is the fraudulent attempt to steal user data such as login credentials, credit card information, or even money using social engineering techniques. **This type of attack is usually launched through e-mail messages, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL.** A targeted form of phishing called ‘spear phishing’ relies on upfront research on the victims so that the scam appears more authentic, thereby, making it one of the most successful types of attack on enterprises’ networks.¹

An emotional response justifies many people actions when they are phished and is exactly what hackers are looking for. In a training context, that is what a phishing simulation should try to achieve. Training e-mail users is one of the often used measures for preventing phishing, but results are not convincing since threat actors are constantly changing their *modus operandi*. The domain-based message authentication, reporting, and conformance (DMARC) standard ensures that e-mail from fraudulent domains is blocked, diminishing the rate of success of phishing, spoofing and spam² attacks.

In the future, e-mail continues to be the number one mechanism for phishing but not for long. We are already seeing an increase in the use of social media messaging, WhatsApp and others to conduct attacks. The most relevant change will be in the methods used to send the messages, which will become more sophisticated with the adoption of adversarial Artificial Intelligence (AI) to prepare and send the messages. Phishing and spear phishing are major attack vectors of other threats such as unintentional insider threats³.

¹ Phishing
² Domain-based message authentication, reporting, and conformance (DMARC)
³ Artificial Intelligence (AI)
Findings

26.2 billion of losses in 2019 with Business E-mail Compromise (BEC) attacks\textsuperscript{20}

42,8\% of all malicious attachments were Microsoft Office documents\textsuperscript{25}

667\% increase in phishing scams in only 1 month during the COVID-19 pandemic\textsuperscript{2}

30\% of phishing messages were delivered on Mondays\textsuperscript{24}

32,5\% of all the e-mails used the keyword ‘payment’ in the e-mail subject\textsuperscript{28}
Kill chain

Step of Attack Workflow
Width of Purpose
The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION
Most targeted types of services are webmail and software-as-a-service

According to some projections, phishing attacks targeting software-as-a-service (SaaS) and webmail services surpassed those against payment services for the first time in Q1 2019, making them the most targeted sector at 36% of all phishing attacks. This new record follows the trend in 2018 when SaaS and webmail services had just overtaken the financial sector. Although the figure had dropped to 30.8% by the end of 2019, the services mentioned above still remained at the top of the list, with Microsoft 365 services being the phishers’ top target.

Business Email Compromise (BEC) attacks continued to be a problem

A recent study identified that 88% of worldwide organisations experienced spear phishing attacks and 86% of them faced BEC attacks. In 2019, one of the most targeted service was Microsoft 365 and the main focus was on harvesting credentials. Once these credentials had been acquired, the attacker was able to collect more organisational data, a process that could last for weeks or months and could then lead to spear-phishing attacks. The attacker would impersonate an employee, chief executive officer (CEO) or even a trusted supplier to divert funds or re-route payments to third-party accounts. In Q1 2019, companies were targeted by BEC attacks 120% more frequently than a year earlier, resulting in losses as high as US $26.2 billion (ca. €22.2 billion).
More than two thirds of phishing sites adopted HTTPS

There has been a steep increase over the past few years in the number of phishing sites that have adopted HTTPS. In the last quarter of 2019, 74% of phishing sites were using HTTPS, a significant increase compared with just 32% only 2 years earlier. Although technologies such as HTTPS and SSL are designed to secure communications between a client and a server, the presence of a lock in an icon at the browser’s address bar may create the illusion that a website can be trusted.

Threat actors may also use legitimate sites they have hacked to host phishing content, therefore making it challenging for the end-user to identify a site as unsafe. Other factors contributing to the steep rise in HTTPS usage are the plethora of free certificate services such as Let’s Encrypt and the fact that modern browsers mark every HTTPS site as secure, without any further checks.

Phishing target attacks. Source: Proof Point
Phishing-as-a-Service (PhaaS) on the rise

These types of services are typically subscription-based or in the form of a kit, available to download for a fee, and remove the technological barriers to entry, as they allow a less technically skilled individual to carry out a targeted attack. A report from a security researcher identified 5,334 unique phishing kits available by June 2019. What was even more concerning was the relatively low cost of these solutions, around US $50-$80 for a monthly subscription. The same report declared that 87% of the kits included evasion mechanisms such as HTML character encoding and content encryption. Interestingly, some of these services were hosted on legitimate cloud services with proper domain name system (DNS) names and certificates. Statistics from just one of these dark-net marketplaces show how successful these attacks are allowing the attacker or group to steal around 65,000 accounts per month.

Trends in incidents

- There was a change in the effectiveness of phishing attacks using cloud storage, DocuSign, and Microsoft cloud services.
- Impostor attacks include schemes like business e-mail compromise (BEC) and identity deception techniques based on social engineering to make phishing campaigns more effective.
- Microsoft 365 services phishing was the top scheme, but the focus remains on credential harvesting.
- Over 99% of e-mails distributing malware required human intervention - following links, opening documents, accepting security warnings, and other behaviours - to be effective.
Top phishing themes in 2019

- Generic Email Credential Harvesting
- Office 365 Account Phishing
- Financial Institution Phishing
- Microsoft OWA Phishing
- OneDrive Phishing
- American Express Phishing
- Chalbhai Generic Phishing
- Adobe Account Phishing
- Docusign Phishing
- Netflix Phishing
- Dropbox Account Phishing
- LinkedIn Account Phishing
- Apple Account Phishing
- Postal/Shipping Company Phishing
- Microsoft Online Document Phishing (Excel and Word)
- Windows Settings Phishing
- Google Drive Phishing
- PayPal Phishing

Source: Proof Point
Cybercriminals are taking advantage of the public fear of the COVID-19 pandemic, which first appeared in late 2019. It has been reported that phishing attacks involving the virus increased by 667% in a 1-month period (between the end of February 2020 and the end of March 2020), and these types of schemes alone represented a notable 2% of all phishing scams.\(^5\)

New scams involved phishing e-mails designed to look as if they originated from the United States Centre of Disease Control (CDC)\(^6\), the World Health Organisation\(^7\) or even from university health teams\(^8\). They either falsely claimed to showcases of infection in the victim’s area or shared medical experts’ opinions to lure the victim to follow a malicious link. For this reason, the FBI and WHO have issued warnings.\(^8,9\) Because many people in quarantine were working from home, often using outdated security systems\(^11\), cybercriminals were seeking to exploit emerging opportunities and vulnerabilities\(^12\).
ENISA’s response to the COVID-19 pandemic

The outbreak of COVID-19 has brought an immense change in the way we conduct our lives. In this increasingly connected world, we can fortunately continue our professional and private lives virtually. During this unprecedented time, the EU Agency for Cybersecurity (ENISA) shared its cybersecurity recommendations on a variety of topics including working remotely, shopping online, and e-health as well as providing updates on key security advice tailored to the sectors affected. ENISA reviews the threat landscape during the pandemic and produces advice on how to mitigate the risks from the most critical threats. Special attention given to phishing due to the escalation in the number of attacks.

ENISA YouTube video about COVID-19. Source ENISA
Incidents

_Targeted sectors_

The healthcare sector was heavily targeted by phishing (or spear-phishing) attacks in 2019. A security researcher\(^\text{42}\) considered phishing as the main attack vector of the year, through the use of social engineering tactics to deliver e-mails infected with malware\(^\text{2}\) or with links pointing to infected websites. Other sectors were also targeted by phishing attacks such as governments and other public administration entities. For example, in November and December 2019, several diplomats and officials from the Ukrainian government received spear-phishing e-mails directing them to compromised websites.\(^\text{43}\)

_Attack vectors_

Spear phishing remains an extremely prevalent initial access technique used by malicious actors. These use a variety of social engineering tactics to induce recipients to open attachments or navigate to a infected website. Spear-phishing messages typically contain malicious macro-enabled Microsoft Office documents, or a link to such documents. After a user selects ‘Enable Content’, the embedded macro will typically begin the execution of a chain of obfuscated scripts that ultimately results in the download of stage one or dropper malware. JavaScript and PowerShell appear to remain the most popular scripting languages for this purpose.
Examples

A phishing attack to Lancaster University students’ resulted in the loss of personal data.

Hackers phished login credentials of 2500 Discord users.

Online fitness service provider victim of a phishing attack.

Patients affected in UConn Health phishing attack.

A car manufacturer subsidiary lost US $37 million (ca. €31 million) due to a BEC scam.
Proposed actions

- Educate staff to identify fake and malicious e-mails and stay vigilant. Launch simulated phishing campaigns to test organisation's infrastructure as well as the responsiveness of the staff.
- Consider the use of a security e-mail gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Consider applying security solutions that use machine-learning techniques to identify phishing sites in real-time.
- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the mail clients and update them frequently.
- Implement one of the standards for reducing spam e-mails: SPF (Sender Policy Framework)\textsuperscript{34}, DMARC (Domain-based Message Authentication, Reporting & Conformance)\textsuperscript{35} and DKIM (Domain Keys Identified Mail).\textsuperscript{36}
- Ideally, use secure e-mail communication using digital signatures or encryption, for critical financial transactions or when exchanging sensitive information.
- Implement fraud and anomaly detection at the network level for both inbound and outbound e-mails.
- Avoid clicking on random links, especially short links found in social media.
- Do not click on links or download attachments if you are not absolutely confident about the source of an e-mail.
Avoid over-sharing personal information on social media, e.g. duration of absence from office or home, flight information etc. as it is actively used by threat actors to collect information about their targets.

Check the domain name of the websites you visit for typos, especially for sensitive websites, e.g. bank websites. Threat actors usually register fake domains that look similar to legitimate ones and use them to ‘phish’ their targets. Looking only for an HTTPS connection is not enough.

Enable two-factor authentication whenever applicable to prevent account takeovers.

Use a strong and unique password for every online service. Re-using the same password for various services is a serious security issue and should be avoided at all times. Using strong and unique credentials for every online service limits the risk of a potential account takeover to only the affected service. Using a password manager software will make managing the whole set of passwords easier.

When wiring money to an account, double-check the bank recipient’s information through a different medium. Unencrypted and unsigned e-mails should not be trusted, especially for sensitive use-cases such as this.

Check how contact, registration, subscription and feedback forms work on your website and add verification rules if necessary so that they cannot be exploited by attackers.
References


20. “Business Email Compromise The $26 Billion Scam” September 10, 2019. FBI. 

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

https://www.imperva.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service


https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html


34. Open SPF. 
http://www.openspf.org/

35. “Domain-based Message Authentication, Reporting & Conformance “. DMARC. 
https://dmarc.org/
36. "DomainKeys Identified Mail (DKIM)". DKIM. http://www.dkim.org/


46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19
“An emotional response justifies many people actions when they are phished and is exactly what hackers are looking for.”
ENISA Threat Landscape Report
**The year in review**
A summary on the cybersecurity trends for the period between January 2019 and April 2020.

ENISA Threat Landscape Report
**List of Top 15 Threats**
ENISAs’ list of the top 15 threats of the period between January 2019 and April 2020.

ENISA Threat Landscape Report
**Research topics**
Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.
ENISA Threat Landscape Report

**Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

---

**Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

---

**Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.
__The agency__

The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu).

**Contributors**
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and all members of the ENISA CTI Stakeholders Group: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

**Editors**
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

**Contact**
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.