UNHOOKED

Contemporary Web Phishing Attacks That Escape Conventional Security

WHITE PAPER

March 2021

ERMES®
Intelligent Anti Phishing

www.ermes.company

> Rather than fearing or ignoring cyber-attacks, do ensure your cyber resilience to them.

Stéphane Nappo

Global Head Information Security for Société Générale International Banking pole

CONTENTS

1 Overview of Phishing Attacks

Cybercrime is on the rise around the world today.[1] One pernicious form, the "phishing" attack, is reeling in many unsuspecting victims at prodigious rates.[2] The word phishing was coined around 1996 by hackers stealing America Online accounts and passwords. By analogy to the sport of fishing with a rod and line these Internet scammers were using e-mail lures, setting out hooks to "fish" for passwords and financial data from the "sea" of Internet users.[3]

Since then, phishing has grown even more sophisticated and has evolved well beyond just emails. Today, it is largely defined as a fraudulent attempt to obtain sensitive information or data—such as usernames, passwords, and credit card details or other confidential information—by impersonating a trustworthy party in a digital communication. Despite having been around for decades, it is still the most widespread and damaging cyber-attack.

1. See "Cybercrime Expected to Rise at an Unprecedented Rate in 2021," Security Boulevard, December 18, 2020 at https://securityboulevard.com/2020/12/cybercrime-expected-to-rise-at-an-unprecedented-rate-in-2021/. See also "Cybercrime on the Rise: Plotting a Way Forward," Security Magazine, February 5, 2021 at https://www.securitymagazine.com/articles/94527-cybercrime-on-the-rise-plotting-a-way-forward.
2. Google has detected an average of 46,000 new phishing websites every week in 2020. See "Google Registers Record Two Million Phishing Websites In 2020," Forbes, November 25, 2020 at https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/. Also see "Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine," PC Magazine, March 30, 2020 at https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine.
3. Hackers commonly replaced the letter f with "ph," a nod to the original form of hacking known as phone phreaking. Phreaking was coined by John Draper, actually known as Captain Crunch, who created the infamous Blue Box that emitted audible tones for hacking telephone systems in the early 1970s. See "Sidebar: The Origins of Phishing," ComputerWorld, January 19, 2004 at https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html.
4. See generally "Phishing," Wikipedia at https://en.wikipedia.org/wiki/Phishing.

> According to deloitte, the average total cost of a data breach is $3.92m with 90% of data breaches caused by phishing.

The phishing attack is an example of how social engineering[5] techniques can be used to trick the recipient into revealing confidential information through online communications such as email spoofing,[5] instant messaging, text messaging, and links to fake websites where private information is typically collected.

Because hundreds of millions of dollars are transferred through the Internet on a daily basis, businesses and Internet users may be vulnerable to different types of web threats—especially phishing—which may cause significant financial damages, identity theft, loss of private data, brand reputation damage, and loss of customer confidence in e-commerce and online banking.[7]

The phishing attack can also lead to devastating financial losses for businesses that can be further exacerbated by regulatory fines and remediation/legal costs. According to Deloitte, the average total cost of a data breach is $3.92M with 90% of data breaches caused by phishing.[8] Also, 76% of businesses have reported being a victim of a phishing attack.[9]

[5] In a social engineering attack, an attacker uses human interaction (social skills and communications) to obtain or compromise information. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. Attackers often take advantage of current events and certain times of the year, such as natural disasters, health scares, economic concerns, major political elections, and holidays. See "Security Tip ST04-014 – Avoiding Social Engineering and Phishing Attacks," Cybersecurity & Infrastructure Security Agency (CISA), August 25, 2020 at https://us-cert.cisa.gov/ncas/tips/ST04-014.

[6] Email spoofing is a fraudulent email activity that involves hiding the real origins of an email. The act of e-mail spoofing occurs when imposters are able to deliver email by altering the sender information on the email, thus giving the false impression it is coming from a trusted source when it is really not. See "Email Spoofing – What Does Email Spoofing Mean?" Techopedia at https://www.techopedia.com/definition/1664/email-spoofing.

[7] See "Tutorial and Critical Analysis of Phishing Websites Methods," Computer Science Review, Volume 17, August 2015, pages 1-24 at https://www.sciencedirect.com/science/article/abs/pii/S1574013715000039?via%3Dihub.

[8] See "Understanding Phishing Techniques," Deloitte, December 2019 at https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf. The cost of a data breach referenced by Deloitte comes from the Cost of a Data Breach Report published by the Ponemon Institute. Ponemon updated the cost for 2020. It came in slightly smaller at $3.86M. For further details see "Cost of a Data Breach Report 2020," Ponemon Institute, 2020 at https://www.ibm.com/security/digital-assets/cost-data-breach-report/.

[9] Ibid.

Furthermore, when phishing attacks successfully trigger data breaches, phishers can cause untold damage to business reputation and consumer trust.

25%
would trust an organization less if its data were compromised

In Deloitte's General Data Protection Regulation (GDPR) Benchmark survey of 1,650 consumers across 11 countries it was found that 25% would trust an organization less if its data were compromised. Also, 17% of respondents claim they would stop using a service or buying from an organization if a data breach were to occur.[10]

[10] Deloitte's General Data Protection Regulation ("GDPR") survey was based on 1,100 responses from individuals with involvement in GDPR within their organizations and 1,650 responses from consumers. The survey was conducted across 11 countries to get a view on consumer perceptions and organizations' responses to GDPR inside and outside the EU. The countries surveyed were the UK, Spain, Italy, Netherlands, France, Germany, Sweden, USA, Canada, India, and Australia. See report "A New Era for Privacy – GDPR Six Months On," Deloitte, 2018, page 16 at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.

Major Phishing Attack Categories

Currently, there are three major categories of phishing attacks:

- Mimicking Attack
- Forward Attack
- Pop-Up Attack

The **mimicking attack** is where "phishers" typically send a carefully crafted email[11] from what appears to be a legitimate website or well-known institution. It requests victims to confirm, update, or validate their credentials by clicking on a Uniform Resource Locator (URL) link in the email which redirects them to a phony web page that mimicks the legitimate site. This is sometimes referred to as website spoofing or website forgery.[12]

A **forward attack** is where the victim is redirected to a website that asks for the submission of personal information such as credentials, passwords, etc. This information is then passed or sent to phishers at a hostile server. Ultimately, the victim is forwarded to the real website and lulled into a false sense of security that gives the impression that the entire transaction was legitimate.[13]

The **pop-up attack** is a method that urges victims to submit sensitive information by means of a well-designed pop-up window. A widespread example of a pop-up phishing attack is the "pop-up tech support." When browsing the Internet, a victim suddenly receives a pop-up message falsely stating that the user's system is infected with a virus and requests the victim to contact the vendor for technical support.[14]

[11] An attacker can also send a text message that is similar. This is often referred to as a "smishing" attack. It is usually a text containing a hostile link that automatically downloads malware to steal credentials and other confidential information. There are even voice or telephone versions of phishing called "vishing." Ibid.

[12] See "Phishing and Spoofing," Phishing.org at https://www.phishing.org/phishing-and-spoofing.

[13] This type of phishing attack is also referred to as "cross-site scripting." An attacker finds a well-regarded Web site containing a page that is vulnerable to an attack. The attacker crafts a special URL that points to this Web page while inserting some of the attacker's own content into the page. This content could consist of a form that queries a user for credentials such as passwords, credit card numbers, etc. It then passes or forwards those values back to the attacker. The result is that the user is lulled into a false sense of security since he trusts the site and therefore trusts any transaction he has with it, even though in reality he is transacting with an attacker. See "Phishing and Cross-Site Scripting," Broadcom at https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument.

[14] See "How to Spot, Avoid and Report Tech Support Scams," U.S. Federal Trade Commission (FTC) at https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

A popular variant of this attack is known as "in-session phishing." It displays a pop-up window during a web browsing session that pretends to have been opened from the targeted session. This pop-up window, which the user now believes to be part of the targeted session, is then used to steal user data in the same way as with other phishing attacks.[15]

An example of an in-session phishing attack might be a pop-up window that shows up during an online banking session asking the victim to retype a username and password while falsely stating that the "session has expired." The victim enters these details, not expecting the pop-up to be fraudelent because they had already logged into the bank's website.

PHISHING ATTACK CATEGORIES

MIMICKING ATTACK

Redirection to a phony web page that mimics the look of a legitimate website.

FORWARD ATTACK

Victim sent to a fake web page, information collected, redirected to real website.

POP-UP ATTACK

A method that urges victims to submit information by means of a pop-up window.

[15] See generally "In-Session Phishing," Wikipedia at https://en.wikipedia.org/wiki/In-session_phishing.

2 Common Phishing Attack Methods

There are several common phishing methods or techniques that comprise the bulk of most attacks occurring around the world today. These tactics or methodologies generally fall into three groups: impersonation, cloaking, and obfuscation. Moreover, these tactics can be combined with one another when delivering a single attack.

Impersonation

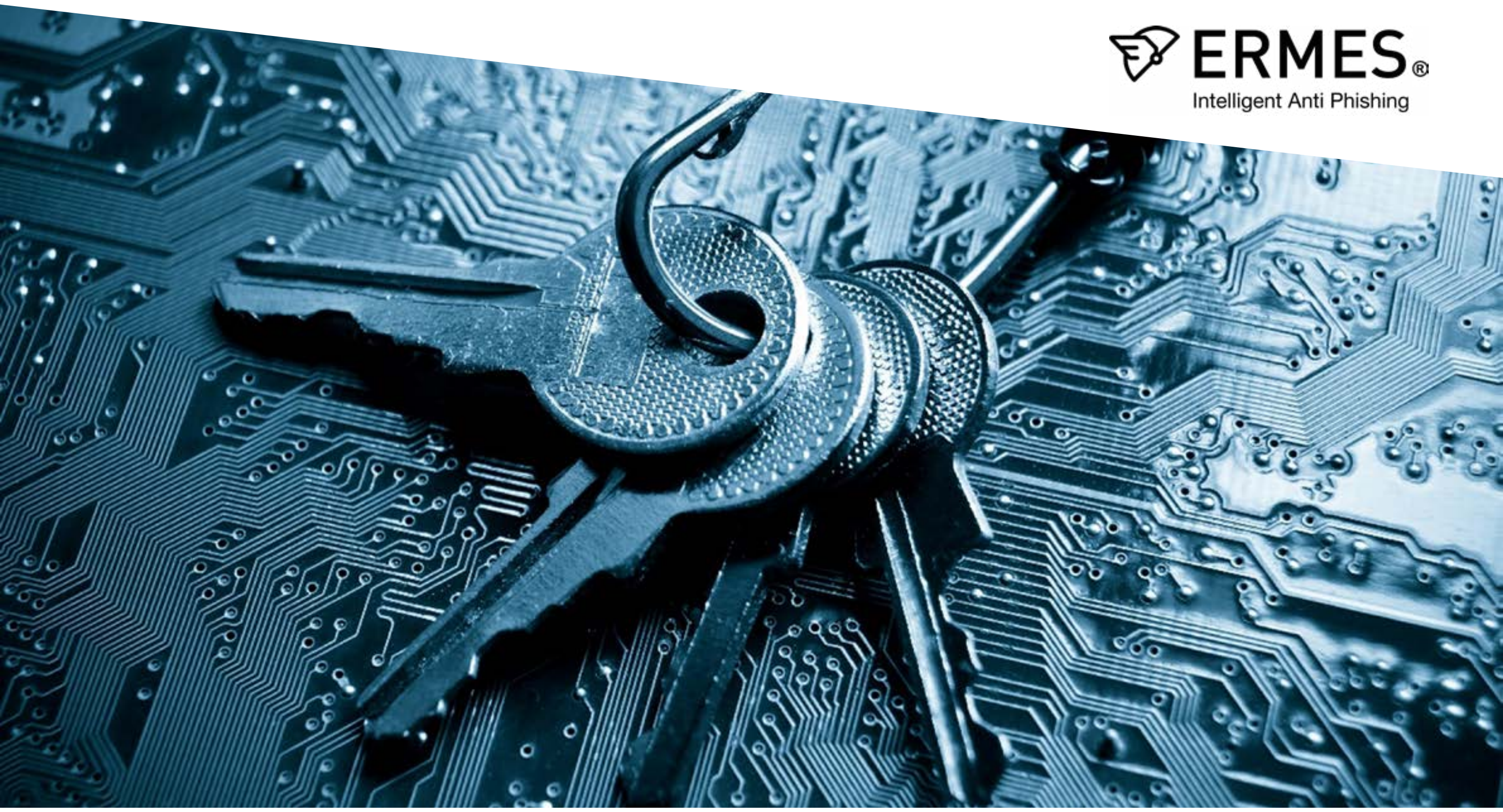
Impersonation tactics mostly rely on URL link manipulation to trick a user into believing they are clicking on or being directed to a trusted website or domain when they are really not. Instead, a purposefully engineered link directs the victim to a counterfeit or malicious website to phish for sensitive information. Impersonation techniques are frequently used in the mimicking attacks and forward attacks previously discussed.

Basically, these dubious URL links impersonate the real domains of legitimate organizations and brands.

Several popular impersonation techniques used by phishers today to intentionally mislead users include:

- Typosquatting
- Bitsquatting
- Combosquatting
- Homographs
- Sub-Domain Impersonation

Typosquatting, also known as URL hijacking, is a form of cybersquatting and brandsquatting—sitting on sites of another brand or copyright—that targets Internet users who incorrectly type a website address into their web browser (i.e., “Gooogle.com” instead of “Google.com”).



When users make such a typographical error, they may be led to an alternative website owned by a phisher that is usually designed for malicious purposes.

The term **bitsquatting** has also been used to describe this tactic. It involves registering a domain name one bit (or one key press) different than the legitimate domain.

Combosquatting is another URL impersonation technique that does not involve typos or misspellings. Instead, it relies on attackers registering domain names that add or combine a small string of characters to the real URL they are targeting—typically in the form of a prefix or suffix.

For example, phishers could register www.yourbankname-security.com or www.security-yourbankname.com tricking a user who may have just glanced to make sure that the bank name is there without detecting the subtle change.

16. See "What is Typosquatting," McAfee, July 3, 2013 at https://www.mcafee.com/blogs/consumer/what-is-typosquatting/.
17. See "Bitsquatting: DNS Hijacking Without Exploitation," Dinaburg at http://dinaburg.org/bitsquatting.
18. See "What Is Combosquatting and How It Can Trick You into Trusting Malicious URLs," Wccftech, October 31, 2017 at https://wccftech.com/combosquatting-trick-users-trust-malicious-urls/.

An extremely surreptitious technique used to confuse a legitimate website with a fake domain name is the **homograph** attack. Homograph attacks exploit confusable characters to obtain a domain name that is hard to distinguish from the original target name. One of the simpler uses of this technique is to use numbers in place of similar letters as done by bl00mberg.com or g00gle.com. While this technique is easily spotted as in these examples, this is not always the case.

Since its inception, Internationalized Domain Names (IDNs) have allowed for non-Latin characters to be entered into domain names. This feature has led to attackers forging malicious domains by using non-Latin character sets—such as Greek or Cyrillic glyphs—which appear nearly identical to their Latin counterparts[19].

The following example is a homograph of the Google domain that appears identical and indecipherable in all aspects from the real domain: *google.com*. In this case, the Latin small letter O was swapped with the Greek small letter Omicron.[20]

Basically, a homograph attack is a method of deception where an attacker leverages on the similarities of character scripts to create and register phony domains of existing ones to fool users and lure them into visiting.[21]

Lastly, **sub-domain impersonation** or domain spoofing may have several variant methods, but a popular version that exploits the use of sub-domain names provides a clear example. It works like this—a phisher registers a domain name such as com-signin.id. The attacker then prepends a sub-domain to the front of the registered domain with an established and trusted brand such as Apple. The full URL now looks like this: *apple.com-signin.id*.

[19] See "The 2017 Homograph Browser Attack Mitigation Survey," Australian Information Management Security Conference at https://ro.ecu.edu.au/ism/210/.

[20] To see that this is not the real Google domain, try copying and pasting this URL for google.com into the address bar of a web browser. It will not be directed to Google's website.

[21] For further understanding of homographs see "Keep Your Eyes Peeled for PUNY Code Attacks!" Ermes at https://www.ermes.company/keep-your-eyes-peeled/.

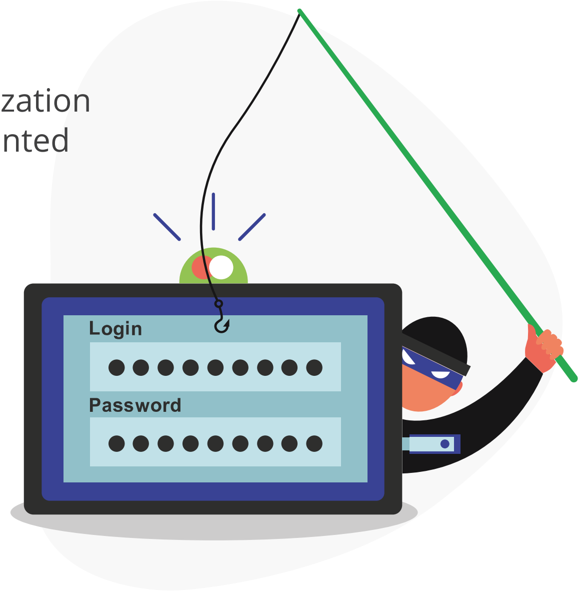
This trick of targeting or using a trusted brand name (Apple) as a sub-domain of another website (com-signin.id) can easily mislead users. Once the link is clicked on, it takes a user to another website that can easily spoof Apple's brand to phish for the user's Apple credentials and password.[22] This tactic has also been referred to as target embedding [23].

Another trick that is also being deployed in the above example is the use of a highly unpopular top-level domain (TLD) name such as ".id" to further confuse the user. There are 1,500+ TLD names[24] that could be potentially used to target well-known websites. Examples might include: ".online" or ".bid" or ".pw" from among the many available. To illustrate their possible use to mislead people that are not carefully scrutinizing links to websites, here are a few examples—paypal.online, ebay.bid, or amazon.pw.

Cloaking

Cloaking is mostly a "black hat" search engine optimization (SEO) technique in which the web page content presented to a search engine spider or crawler, such as Google's Googlebot, is different from that presented to a user's browser when the page is actually viewed.

Basically, it is a tactic used by phishers to deceive search engines into displaying a page when it would not otherwise be displayed in the search engine results. This method is frequently used to trick search engine users into visiting a site that is substantially different from the description shown in the search engine results page.



As mentioned earlier, malicious websites often mimic top brands to host malware and launch phishing attacks to collect user credentials.

[22] For more examples of sub-domain phishing attacks see generally "Snowshoe Spamming Brings Scale to Savvy Subdomain Phishing Attacks," Proofpoint, February 9, 2017 at https://www.proofpoint.com/us/threat-insight/post/snowshoe-spamming-brings-scale-savvy-subdomain-phishing-attacks.

[23] See "You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates," CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019 Proceeding at https://dl.acm.org/doi/10.1145/3319535.3363188.

[24] To view the current list of TLDS at the Internet Assigned Numbers Authority (IANA), see "IANA's List of TLDs in Machine-Readable Format," IANA at https://data.iana.org/TLD/tlds-alpha-by-domain.txt.

[25] See generally "On Cloaking Behaviors of Malicious Websites," Computers & Security, Volume 101, February 2021 at https://www.sciencedirect.com/science/article/pii/S0167404820303874?via%3Dihub.

[26] Ibid.

These phishing sites frequently attempt to hide malicious content from search engine crawlers but show the harmful content to users through client browsers.[27] In other words, the cloaking technique is used by phishing websites to hide their malicious content from crawlers to avoid blacklisting as much as possible while increasing their lifespan. For this reason, cloaking has become one of the most common approaches used by phishing websites to avoid detection and recognition as a threat.

Obfuscation

Obfuscation is the act of making something obscure, unclear, or unintelligible. Phishers frequently attempt to obfuscate the code and content on malicious web pages using techniques that incorporate two methods: code obfuscation and image-based obfuscation.

Both of these methods can be deployed individually or in tandem to deceive victims. Additionally, obfuscation is used for the purpose of hiding malicious code to deceive phishing-detection algorithms. In other words, obfuscation can involve writing code that is intentionally hard to read, usually to prevent the code of an attack from being easily discovered or analyzed.

[27] Ibid.

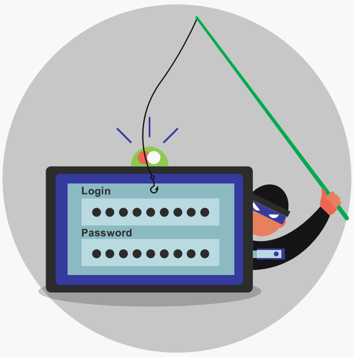
An example of obfuscation might involve an attacker taking a screenshot of a target website, perhaps a popular bank or financial institution, and using it as the background image for a malicious phishing website. Then the phisher will use code to overlay a phony login form on top of the image to collect user credentials and passwords to gain access to bank accounts.

Increasingly, phishers are also turning to software sold on the black market or even open sourced that allows attackers with relatively few skills to launch malicious campaigns at scale. These "phishing kits" provide most of the necessary components including development environments, graphics, and code to create passable copies of legitimate websites. These kits are sophisticated and the landing pages to which users are directed via email, pop-ups, social media, etc. are obfuscated to avoid detection by endpoints and gateways[28].

COMMON PHISHING ATTACK METHODS

IMPERSONATION

Tactics that mostly rely on URL manipulation to deceive a user into clicking a hostile link.



CLOAKING

"Black hat" SEO technique where web page content is different than what is submitted to search engine crawler.

OBFUSCATION

Hiding or obfuscating the content of malicious web pages using images and code.

[28] See generally "Hiding in Plain Sight: Obfuscation Techniques in Phishing Attacks," Proofpoint, https://www.proofpoint.com/sites/default/files/proofpoint-obfuscation-techniques-phishing-attacks-threat-in-sight-en-v1.pdf.

3 Fast-Paced Phishing Campaigns

Because of the difficulty of operating a phishing website for long periods undetected, there is now a common trend among attackers to create websites that are designed to be active online for only short intervals. During this time, phishers will attempt to deceive as many victims as possible without detection.

Phishers have become very nimble in their approach. About 84% of phishing sites exist for less than 24 hours, with an average life cycle of under 15 hours. There are even some cases where the site is active for as little as 15 minutes.[29]

“Phishers have become very nimble in their approach. About 84% of phishing sites exist for less than 24 hours, with an average life cycle of under 15 hours. There are even some cases where the site is active for as little as 15 minutes.”

The short lifecycle of these phishing sites makes them extremely dangerous because there is generally not enough time for these sites to be analyzed and placed in the appropriate databases and blacklists. Unfortunately, because these sites are so new and recent, many vulnerable users will get deceived.

[29] See “84% of Phishing Sites Last for Less Than 24 Hours,” Infosecurity Magazine, December 12, 2016 at https://www.infosecurity-magazine.com/news/84-of-phishing-sites-last-for-less/.

To get a real sense of how many of these malicious sites are out there, Google registered a record number of more than 2 million phishing websites in 2020 according to data analyzed by Atlas VPN.[30]

2,000,000

PHISHING WEBSITES IN 2020

The tech giant also detected an average of 46,000 new phishing websites every week in 2020. These numbers represents a 19.9% increase compared to all of 2019, indicating the extent to which the coronavirus pandemic has boosted the opportunity for online scams.[31]

To make matters worse, when a phishing campaign has been successful in accessing sensitive information, such as credentials and passwords, this "leakage" of confidential data can attract multiple attackers. Credential sharing between attackers has become a commonly observed activity.[32] The timeframe for this exploitation is typically anywhere from an hour to 1-2 days from the leakage.[33] Usually, the attackers log in from different countries than where the original phishing site was located.[34]

[30] See "Google Registers Record Two Million Phishing Websites In 2020," Forbes, November 25, 2020 at https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/.

[31] Ibid.

[32] See "What Happens After You Leak Your Password: Understanding Credential Sharing on Phishing Sites," Asia CCS '19: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019 Proceeding at https://dl.acm.org/doi/10.1145/3321705.3329818.

[33] Ibid.

[34] Ibid.

4 Public Key Certificates

There is a common misperception among Internet users that any website that has the "padlock" icon indicator in a browser address bar or an "https" at the beginning of a URL indicates whether it is a legitimate e-commerce site or a phishing trap. Unfortunately, nothing could be further from the truth.

These indicators only mean that a browser was able to authenticate a website's public key or digital certificate that was issued by a certificate authority (frequently referred to as a CA).[35] It does not necessarily mean or represent that the content of a website is really what a user expects it to be.

These certificates merely signify that the data being transmitted back and forth between a browser and a website is encrypted and cannot be read by third parties. The presence of the padlock does not mean the site is legitimate, nor is it any proof the site has been security-hardened against intrusion from phishers.

Today, it has gotten much easier to obtain a public key certificate through free certificate authorities like "Let's Encrypt," a non-profit run by the Internet Security Research Group.[36] It is an open and automated organization that provides millions of certificates.[37] Accordingly, many phishing websites can now easily obtain their own public key certificates through this or similar organizations.

The number of phishing websites using a public key certificate has continually increased over the last several years.[38] Now, as a consequence, simply checking to see whether a website has a certificate is no longer effective when it comes to detecting phishing websites.

[35] A digital certificate is an electronic document used to prove the ownership of a public key for the purposes of encrypting sensitive data. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. See generally "Public Key Certificate," Wikipedia at https://en.wikipedia.org/wiki/Public_key_certificate.

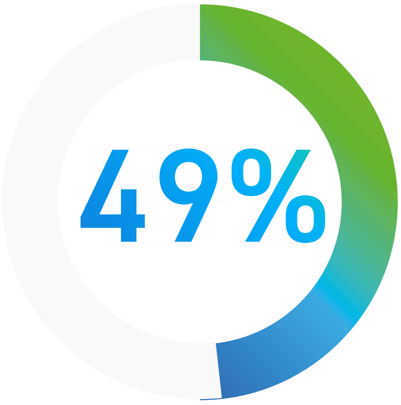
[36] For further information see generally https://letsencrypt.org/.

[37] The purpose of which is to help advance HTTPS adoption to the entire web. Currently, it is the world's largest provider of valid certificates. As of November 2020, it serves 232 million websites with 144 million active certificates. See the 2020 Annual Report, Let's Encrypt at https://www.abetterinternet.org/documents/2020-ISRG-Annual-Report.pdf.

[38] See "Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites," SOUPS'19: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security, 2019 Proceeding at https://dl.acm.org/doi/10.5555/3361476.3361491.

Moreover, it is has generally become impossible to differentiate between benign sites and phishing sites based solely on the content of their certificates.[39] New research also indicates that nearly half (49%) of all phishing scams are now hosted on sites whose Internet address includes the padlock and begins with "https."[40]

Ermes Cyber Security even conducted a study during the first half of 2019 using a dataset comprised of over 240,000 domains with a public key certificate—36% of them were found to be malicious.



OF PHISHING SCAMS ON SITES WITH THE PADLOCK & HTTPS

[39] Ibid.

[40] See "Half of all Phishing Sites Now Have the Padlock," Krebs on Security, November 2018 at https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/comment-page-1/

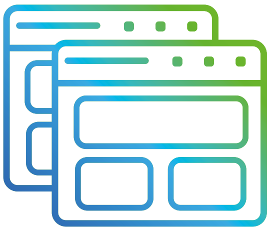
5 Conclusion

Phishing attacks are on the rise around the world today—

- These attacks can lead to devastating financial losses for businesses that can be further exacerbated by regulatory fines and significant remediation costs.

- When a phishing attack successfully triggers a data breach, it can also cause untold damage to business reputation and consumer trust.

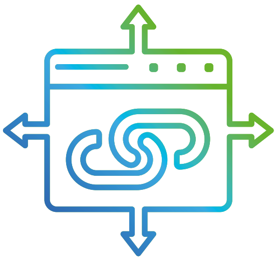
- There are multiple phishing attack categories and several methodologies making it increasingly more difficult for businesses using traditional security to effectively detect them and stop them in their tracks.



- Major phishing attack categories include the mimicking attack, forward attack, and pop-up attack.

- The mimicking attack typically involves sending an unsuspecting user an email that includes a link which redirects the user to a phony web page that mimicks a legitimate site to phish for sensitive information.

- The forward attack is where the victim is redirected to a website that asks for the submission of personal information such as credentials, passwords, etc. This information is then passed or sent to phishers at a hostile server. Afterward, the victim is forwarded to the real website.



- The pop-up attack is a method that urges victims to submit sensitive information by means of a well-designed pop-up window.

- There are several common phishing methods or techniques that comprise the bulk of most attacks occurring around the world today. These tactics or methodologies generally fall into three groups: impersonation, cloaking, and obfuscation. These tactics can also be combined with one another when delivering a single attack.

- Impersonation tactics mostly rely on URL link manipulation to trick a user into believing they are clicking on or being directed to a trusted website or domain when they are really not.

- Cloaking is mostly a “black hat” search engine optimization (SEO) technique in which the web page content presented to a search engine spider or crawler, such as Google’s Googlebot, is different from that presented to a user’s browser when the page is actually viewed.
- Phishers frequently attempt to obfuscate the code and content on malicious web pages using techniques that incorporate two methods: code obfuscation and image-based obfuscation. Both of these methods can be deployed individually or in tandem to deceive victims.

- The short lifecycle and fast-paced nature of many of these phishing campaigns does not generally provide enough time for these sites to be properly analyzed and placed on blacklists. This only makes the situation more dire and dangerous for businesses.

- Phishers have become very nimble in their approach. About 84% of phishing sites exist for less than 24 hours, with an average life cycle of under 15 hours. There are even some cases where the site is active for as little as 15 minutes.
- When a phishing campaign has been successful in accessing sensitive information, such as credentials and passwords, there is usually “leakage” of confidential data that can attract multiple attackers. This usually occurs within an hour or 1-2 days. Attacks typically originate from different countries.
- Nearly half (49%) of all phishing sites possess public key certificates that give users and businesses a false sense of security.
- It has generally become impossible to differentiate between benign sites and phishing sites based solely on the content of their certificates.

Based on these key takeaways and insights about the impending dangers of contemporary phishing attacks, it is evident that relying exclusively on traditional corporate security solutions such as endpoint protection, network filtering, and EDR do not provide enough protection against phishing.

Today, these attacks are extremely fast-paced and short-lived. They can cause untold damages very quickly—before they are even detected by traditional security solutions. Most of these phishing websites have such a short lifespan that there is not enough time to blacklist them. So, they never become a "known" threat and remain invisible to these traditional solutions.

Ermes has developed an architecture that uses artificial intelligence/deep-learning to detect these contemporary types of phishing threats. This technology further fortifies enterprises from being victimized by evolving and proliferating phishing attacks that are fast and short-lived.

If your organization would like to learn more about how artificial intelligence and deep learning can be effectively put to use to stop contemporary phishing attacks that normally elude traditional security, please contact us at www.ermes.company or info@ermes.company.

> In the world of cyber security, the last thing you want is to have a target painted on you.

Tim Cook
CEO, Apple

About

Ermes–Intelligent Anti Phishing is the first on-device web protection solution that can avoid people-centered web attacks before they even occur. Any company can easily activate Ermes protection by providing users with a private, fast, and safe navigation experience through both PC and mobile devices wherever they are located. This simple stand-alone solution is fully compatible with any cyber-ecosystem and allows companies to immediately activate web browsing protection in a matter of minutes.

Because Ermes technology is based on artificial intelligence and deep learning, it is able to detect web requests that are not authorized by the user. Specifically, it can detect surreptitious and potentially dangerous web requests—even those that are ultimately directed to a well-known website—unlike traditional security solutions.

Using completely proactive architecture—unlike the reactive nature of traditional solutions—Ermes has blocked 360+ billion connections and protected 30K+ people to date by providing unique and advanced solutions aimed at disrupting cyber-attacks that continue to evade traditional security.

We look forward to working with you so we can demonstrate the security and performance benefits that our complementary system can provide to your organization.

Contact

Ermes Cyber Security S.R.L.
Corso Bernardino Telesio 29,
10146 Torino, Italy

info@ermes.company

www.ermes.company