# PREVENTING PHISHING ATTACKS IN THE NEW NORMAL

# Introduction

As millions of employees transitioned to remote work, hackers have not missed the opportunity to capitalize on the fear, worry, and anxiety that people naturally felt about the outbreak. When the pandemic began, Google was detecting[1] 18 million coronavirus-themed malware and pushing emails per day. According to the Anti-Phishing Working Group,[2] the number of phishing attacks has only grown since then.

Phishing threats in the current cyber landscape are frightening for organizations and employees. From the upsurge in COVID-19-related malicious domains to the use of fraudulent advertisements offering vaccines for sale, organizations have seen an unprecedented increase in the sophistication and volume of cyber exploits. These attacks have sought to spread malware and compromise personal data.

As the biological pandemic continues, so does the targeting of healthcare organizations, seeking to steal valuable commercial and personal information. Such attacks have even disrupted vital research operations. Since November 2020,[3] there has been an increase of over 45 percent in the number of attacks seen against healthcare organizations globally, compared to an average 22 percent increase in attacks in other sectors.

> "Phishing targeting webmail and Software-as-a-Service (SaaS) endures as the largest phishing category, with 31.4 percent of all attacks." *– Anti-Phishing Working Group*

Phishing schemes work well because people can make mistakes. Well-crafted socially engineered phishing attacks are successful when people  fail to detect the scam. It's estimated[4] that over 90 percent of all attempted cyber attacks result from phishing, and 32 percent of actual data breaches involved phishing activity. Thus, preventing phishing attacks should be an organization's top cyber security priority.

In this whitepaper, we'll discuss the most popular phishing attacks that hackers are using during the pandemic and how to recognize them. At the end, we'll provide our recommendations to prevent phishing attacks.

[1] ""Findings on COVID-19 and online security threats," Google, Shane Huntley, April 22, 2020

[2] ""Phishing Activity Trends Reports," Anti-Phishing Working Group, 2020

[3] ""Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again," Check Point Software, January 5, 2021

[4] ""Google and Amazon overtake Apple as most imitated brands for phishing in Q2 2020," Check Point Software, August 4, 2020

# E-mail Phishing

E-mail-based phishing attacks saw the highest increase compared to any other phishing attacks during the pandemic. According to Check Point's Brand Phishing Report,  the increase in phishing emails was one of the most prominent trends of the work-from-home era. Cyber criminals are well aware of the distractions people are dealing with while working remotely.

In a phishing e-mail, the scammer tricks the victim into thinking they're receiving a legitimate e-mail from a legitimate sender. These attacks frequently rely on spoofing, in which the e-mail header, or 'from' field, is forged to look as if a trusted person sent the e-mail.

Phishing emails often convey a sense of urgency – an urgent deadline, a fine, or a loss of funds or a job. The email might suggest you'll miss out on a reward, raising your curiosity. If users feel pressured or unsure in any way then not clicking is the desired course of action.

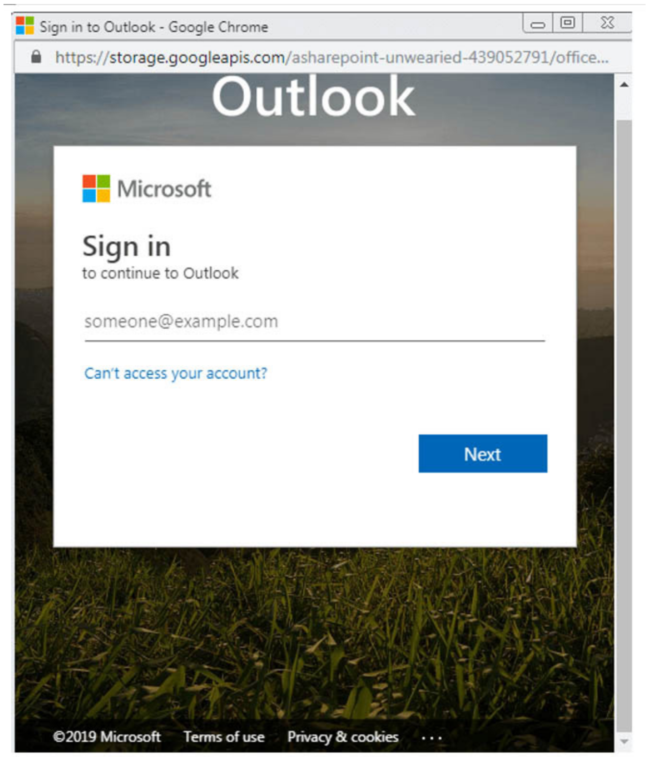
There are five types of e-mail phishing attacks that threat actors can deploy: credential stealers, malicious documents, exploit kits, clone phishing, and spear phishing. We'll look at each.

## CREDENTIAL STEALERS

This is viewed as an attacker's "bread and butter" method.  It's one of the easiest attacks to deploy, and it's effective.

An e-mail deploying a credential stealer often includes a link which takes you to a fake website. In Check Point's Brand Phishing Report,  Microsoft was the most imitated brand in phishing attempts. Clicking on a link in a phishing e-mail may have included this web page.

Notice that the site is hosted on googleapis.com, and not microsoft.com or outlook.com. By using a well-known public cloud service such as Google Cloud to host their phishing pages, hackers can improve their chances of executing a successful phishing attack.


Sign in to Outlook - Google Chrome
https://storage.googleapis.com/asharepoint-unwearied-439052791/office...
Outlook
Microsoft
Sign in
to continue to Outlook
someone@example.com
Can't access your account?
Next
©2019 Microsoft
Terms of use
Privacy & cookies
...

[5] "“Microsoft is Most Imitated Brand for Phishing Attempts in Q3 2020," Check Point Software, October 18, 2020

[6] "Ibid, 2

To stay protected against this attack, employees must be cautious of lookalike domains and spelling errors in websites or the domain. They must also be wary of the domain name not matching the content of the page. In this case, the domain should have been a Microsoft domain, not a Google domain.

> "It must be said that hacking and even breaches in general (at least in our dataset) are driven by credential theft. Over 80% of breaches within hacking involve brute force or the use of lost or stolen credentials." *– Verizon's 2020 DBIR*

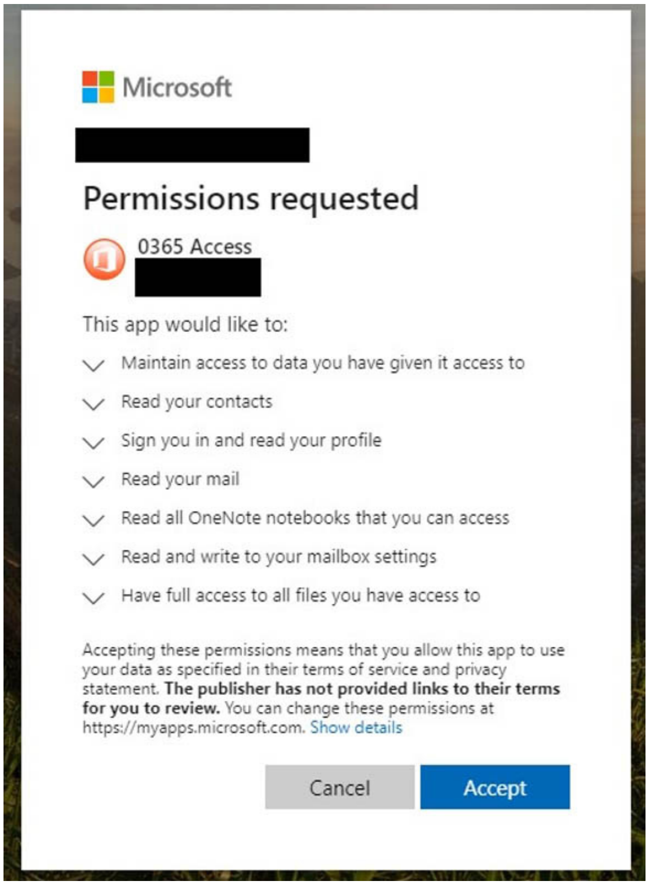
## CONSENT PHISHING

In this type of phishing attack, hackers trick their victims into granting a malicious app permission to access sensitive data.

According to Microsoft,[7] scammers have sent phishing emails targeting business executives with COVID-19 bonus promises. The hackers sent millions of phishing emails targeting chief executives and senior managers in both private and public companies. When victims clicked the malicious link, a prompt displayed asking the victim to sign off on privileges including the ability to read emails and change email settings.

When victims clicked the malicious link, a prompt displayed asking the victim to sign off on privileges including the ability to read emails and change email settings.

If the victim grants access, the phishing attack paves the way for hackers to launch malicious schemes, such as tricking employees into wiring money for simply viewing sensitive company data.



Microsoft

[redacted]

Permissions requested

0365 Access
[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

*Source: Microsoft*

[7] ""Hackers Try to Phish Business Executives With COVID-19 Bonus Promise," PCMag, Michael Kan, July 7, 2020.

## EXPLOIT KIT

On a global scale, threat actors are continuing to have success with exploit kits[8] in the current landscape. This is how an exploit kit works: the victim opens the email, clicks on the link to a malicious page, and at that point, if the user's device or browser is out of date, the exploit kit will use known vulnerabilities to exploit that user's machine. You typically won't see zero-days in an exploit kit, since exploit kits possess a collection of older vulnerabilities that have been known for months or years. However, exploit kits are effective in compromising devices, and just like the malicious document, they can steal passwords, and install a backdoor or install ransomware.

## SPEAR PHISHING

Phishing attacks can be categorized as "spear phishing," which simply refers to a criminal who specifically targets an individual or an organization. In contrast, bulk phishing relies on sending a mass-market e-mail, which increases the volume of e-mails sent but has a lower success rate because it's not tailored to the individual receiving it. Attackers also typically go after high-value victims and organizations, such as those holding a C-level job title.

Spear phishing is often successful because the attackers spend time to research the intended target, such as referencing an event the recipient may have just attended or discussing a trending topic in the recipient's industry. These socially engineered e-mails may also appear to come from the victim's boss or coworker, tricking the recipient into making a financial transaction or divulging sensitive data.

As the pandemic continues, healthcare executives[9] have received these spear phishing emails, including UMass Memorial Healthcare CEO Dr. Erick Dickson, Holyoke Medical Center CEO Spiros Hatiras, and others.

## CLONE PHISHING

Clone phishing is a type of phishing attack where the threat actor copies a legitimate email message that was sent by a trusted company. The tainted email replaces or adds links that redirect to a malicious website. Hackers also typically spoof the e-mail address.

The attacker will typically explain why the victim is receiving the same message by saying that it's an updated version of the e-mail.  Because the victim may have already seen the previous, legitimate message, they're more likely to fall for the scam.

Security training needs to emphasize that employees double check the supposed sender to confirm their identity when receiving a message that seems "off" in its lingo, grammar, or offering.

[8] ""A View of COVID-19's First Wave of Cybersecurity," Info-Security Magazine, David Gray, June 17, 2020.

[9] ""Hospitals said to tighten email security in response to CEO spear phishing attempts," HealthcareITNews, Kat Jercich, November 5, 2020.

## VISHING

Vishing, or voice phishing by phone, targets individuals to get them to divulge sensitive information or credentials during the call. In August 2020, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory warning about a wave of vishing attacks targeting US private sector companies.

According to KrebsOnSecurity,[10] cyber criminals have offered vishing attacks as a marketplace service. Such services help cyber criminals target a specific company. These criminals have targeted remote employees and attempted to obtain their VPN credentials in order to infiltrate the corporate network.

> "Before the pandemic and the sudden increase in remote workforces, vishing scams were not uncommon. However, since July 2020, vishing scams have evolved into coordinated and sophisticated campaigns aimed at obtaining a company's confidential, proprietary and trade-secret information through the company's VPN with the help of the company's own employees."
>
> *– Kevin Cloutier, Partner, Sheppard Mullin*

Many cyber criminals are using the COVID-19 pandemic masquerading as a government official, make illegal health care pitches, among other approaches. They may also offer fake tax refunds or claim to help with unemployment compensation, looking for a way to steal personal information, hack into secure systems, and possibly compromise the organization that employs the victim.

Let's not forget: one of the most successful vishing attacks occurred in July 2020, in which Twitter suffered a breach and hackers gained access to high-profile Twitter accounts belonging to Barack Obama, Joe Biden, Elon Musk, Jeff Bezos, and others. The hackers tweeted bitcoin requests which garnered over $100,000 in a few hours, before it was discovered that the attack stemmed from a vishing attack that persuaded Twitter employees to give up access to internal Twitter tools.

[10] "Voice Phishers Targeting Corporate VPNs," Brian Krebs, KrebsonSecurity, August 19, 2020.

Hackers can even use AI voice technology [11] to spoof the voice of a high-level executive within your company. That's exactly what happened to the CEO of a UK-based energy company who believed he was talking to his boss on the phone, the chief executive of the firm's German parent company. He fell victim to the trick and wired $243,000 to the bank account of the Hungarian scammer.

To prevent a successful vishing attack, employees should never give out personal information over the phone, unless they're 100% certain they know who they're speaking to. Also, people should never agree to conduct wire transfers to virtual payments to unfamiliar people. Finally, suspicious calls should be reported to your IT department as soon as possible.

## SMS PHISHING

SMS phishing is a vector attackers use to send text messages that appear to come from legitimate companies. These phishing messages convince the recipient to download a malicious app, provide sensitive details, or click on a malicious URL. Phishers use SMS spoofing techniques to make the phone number appear that it's coming from a legitimate organization. These attacks are becoming increasingly more common, as one study [12] reported a 29% growth in smishing between March and July of 2020.

> "Criminals love Smishing because users tend to trust text messages, as opposed to email, of which people are naturally more suspicious." *– John Kronick, Journalist*

These attacks are often more successful than e-mail phishing attacks because people are less wary of suspicious messages on their phones than ones on their PCs. A text message is more intimate than an e-mail sent to a corporate e-mail account, and personal devices typically lack the security available on corporate computers. Furthermore,[13] 98 percent of text messages are read and 45 percent are responded to, while the numbers for e-mails are 20 percent and 6 percent, respectively.

To prevent successful smishing attacks, employees should remain cautious of texts containing unnatural language or grammatical errors. If an offer seems to be too good to be true, it just might be. Finally, employees should avoid clicking on links or downloading apps from a text message.

[11] "A Voice Deepfake Was Used To Scam a CEO Out Of $243,000," Forbes, Jesse Damiani, September 3, 2019.

[12] "Catches of the month: Phishing scams for October 2020," ITGovernance, Luke Irwin, October 7, 2020..

[13] "Tap Into The Marketing Power of SMS," Gartner, Chris Pemberton, November 3, 2016.

# Phishing Prevention Strategies

Adopting the following anti-phishing strategies can help drastically reduce your organization's exposure to phishing threats:

## 1. EDUCATE YOUR EMPLOYEES

Training users on how to identify and avoid potential phishing attacks is critical. However, sending an awareness e-mail is not sufficient since many employees may be too busy or distracted to read through the entire e-mail.  Research firm USENIX [14] discovered that a phishing awareness program significantly improves the ability of employees to directly identify phishing and legitimate emails. The investigation also found that video and interactive training examples outperformed text tutorials.

Consider issuing a mandatory training program to ensure your employees can correctly identify phishing threats. In your training program, provide exposure to the most relevant and malicious phishing messages. Maximize user engagement by implementing interactive training modules and videos. Track the results of your assessments to help you determine which phishing simulation to send next in order to better educate your users. You'll also want to train employees to report any suspected phishing emails, so the IT team can take action to delete malicious emails before they are opened.

Add phishing simulation to your phishing awareness program to help your employees detect malicious emails. For example, send a phishing simulation email to all your employees once per month. Make the email appear to come from an IT department, Slack, Zoom, or any other vendors you use. Those who respond or comply with the email should receive an immediate response and directed to a "Red Flags" page, explaining the red flags in the specific phishing email and how not to fall for it again.

The goal of the simulation is education, not punishment. Make sure your employees are aware that the results are confidential.

## 2. REVIEW YOUR SECURITY PASSWORDS

Cyber criminals commonly target user credentials. If an attacker steals an employee password, it's much more difficult for the organization to detect nefarious behavior. Here are several best practices to implement regarding passwords:

[14] ""The Benefits of Using Phishing Simulations," The Defence Works, January 25, 2019.

- Implement a policy that requires unique, strong passwords across multiple accounts. Otherwise, threat actors can break into multiple accounts using the same password. It's estimated the 73 percent of online accounts reuse the same password, so the use of unique passwords can greatly reduce the chance of compromise.
- Require users to change passwords on a regular basis. Data breaches happen all the time, and if an employee's password.
- Use two-factor authentication. Traditional, password-based authentication systems are more vulnerable to phishing attacks and the use of weak or reused passwords. Two-factor authentication creates an additional level of security for user accounts.

## 3. DEPLOY AN AUTOMATED ANTI-PHISHING SOLUTION

While educating your employees is a necessity, it's not enough by itself. Phishing attacks are becoming extremely sophisticated and can trick even the most veteran cyber security experts. Minimizing the risk of phishing threats requires a technological solution. We recommend an AI-based anti-phishing solution capable of detecting and blocking phishing attacks across all attack vectors. Check Point's anti-phishing solutions includes different products to address different attack vectors– email, endpoint and mobile.

Harmony Email & Office secures inbound, outbound, and internal email from phishing attacks that evade platform-provided solutions and email gateways. It works with other solutions and doesn't require any MX (Mail Exchanger) record changes that broadcast security protocols to hackers. It also analyzes all historical emails in order to determine prior trust relations between the sender and receiver, increasing the likelihood of identifying user impersonation or fraudulent messages. Harmony Email & Office uses artificial intelligence (AI) and indicators of compromise (IoCs) to know what to look for in complex zero-day phishing attacks.

Harmony Endpoint provides anti-phishing for endpoint devices. Its "Zero Phishing" feature identifies and blocks phishing sites in real time and even protects against previously unknown phishing sites. When a user visits a website, the Zero Phishing engine will inspect, identify, and block phishing sites. If the site is considered malicious, then the user will not be able to enter credentials. Zero Phishing also prevents credentials re-use, so users won't expose their corporate passwords on other sites.

Harmony Mobile provides anti-phishing for mobile devices. Zero Phishing allows companies to thwart zero-day phishing threats by inspecting the web page itself and making an informed decision on whether or not it's a phishing site. Combined with the SSL inspection feature, organizations will experience total protection from phishing sites.

# Conclusion

With the increases in phishing attacks during the coronavirus era, you must be aware of what the most popular threats are and how to prevent them. To prevent your organization's data and assets from being compromised, educate your workforce on potential phishing threats, review password security practices, and deploy an automated anti-phishing solution. If you lead cyber security in a healthcare organization, you should be even more stringent with cyber security policies and employee compliance.

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

**www.checkpoint.com**