Devolutions

# The Evolution of Phishing: Why It's Getting Worse & How to Fight Back

## TECHNOLOGY IS NOT ONLY EVOLVING TO MAKE OUR LIVES BETTER— CYBERTHREATS ARE ALSO ADVANCING TO MAKE OUR LIVES WORSE

Recently, my colleague Marc-Olivier looked at some interesting and exciting IT trends in 2021. Unfortunately, technology is not only evolving to make our lives better — cyberthreats are also advancing to make our lives worse. And one of the scariest examples of this is phishing.

Of course, phishing is not a new phenomenon. In fact, it dates all the way back to 1996. But while many trends that emerged at that time have long since entered the dustbin of history, phishing has not only survived, it has surged. Consider the following:

- Nearly 1.5 million new phishing sites are created each month.
- Phishing attacks accounted for more than 80% of reported security incidents in 2020.
- Phishing was the most common type of cybercrime in 2020.
- An analysis of more than 55 million emails shows that 1 in every 99 emails is a phishing attack.

And for those who might have thought — or perhaps hoped — that hackers might have dialed things back during the pandemic, the truth is they accelerated their attacks. For example, in April 2020 Google blocked a whopping 18 million daily malware and phishing emails related to COVID-19. And throughout the pandemic, hackers in the U.S., Canada, UK and elsewhere have regularly impersonated government agencies claiming to offer pandemic-related financial assistance and vaccination/therapy information.

Granted, many phishing attempts these days are not just blatantly obvious, they are often (unintentionally) ridiculous and hilarious. Indeed, we only need to glance at our SPAM folders to see some truly pathetic attempts to steal our personal information. Obviously, we do not have to worry about those. So, why are cybersecurity experts increasingly worried about phishing? Because not all phishing attempts are feeble and easily avoidable. Some are surprisingly subtle and sophisticated, such as:

- Polymorphic phishing
- Phishing that uses HTTPS sites
- Phishing-as-a-service
- Hosting phishing landing pages on public cloud services
- Phishing that uses typo-squatted domain names
- Phishing that uses inverted landing page backgrounds

Let's take a closer look at each of these phishing innovations and see why they are definitely a cause for concern.

## Polymorphic Phishing

Signature-based email security tools scan email elements — such as sender name, sender address, subject line, email body copy, and signature — and compare them against a database of known phishing campaign data. If a match is found, then the email is blocked, flagged, or forwarded to a SPAM folder (depending on how the tool is configured).

Think of it like a bunch of police officers who each have an accurate photo of a wanted criminal. Sooner or later, the officers are going to come across the criminal and take him into custody. But what if that criminal alters their appearance? Then there is a chance they will evade detection. That is essentially what polymorphic phishing tries to do.

Polymorphic phishing changes an email element very slightly that is being scrutinized by signature-based security tools, in an effort to slip through the cracks and ultimately reach victims. For example, if the tool is on the lookout for specific content in the body of an email, hackers will modify it just enough so that the tool does not raise the alarm bell and slam the door shut.

Usually, polymorphic phishing attacks start modestly and target a small group of employees. Once an employee is hooked — i.e., once they mistakenly treat the email as legitimate, often by clicking a link that takes them to a phony login page — hackers use that access to launch broader polymorphic phishing attacks against other employees on the same network.

What makes polymorphic phishing especially devious and deceptive is that once attacks are underway, the compromised accounts cannot be blacklisted — because, as noted above, they all come from the same organization. As more accounts are compromised, it becomes increasingly difficult to contain this type of attack.

## Phishing That Uses HPPTS Sites

Hackers are also increasingly using HTTPS sites to carry out phishing attacks. The logic behind this is simple: many users automatically assume when they see the little lock icon in their browser's address bar that the message they are receiving is trustworthy and safe.

What these users do not grasp is that there are all kinds of free certificate services out there that will grant a website a seal of trust. On top of this, today's browsers mark all HTTPS sites as secure without conducting further checks. While IT and InfoSec professionals realize that there is a whole spectrum of "secure" — ranging from slightly secure to robustly secure — most non-technical users see this as binary: either a site is not secure, or it is secure. And if it has a little lock icon, then it must be 100% secure.

Unfortunately, hackers are counting and preying on this potentially mistaken perception. According to the ENISA Threat Landscape 2020 report, 74% of phishing sites adopted HTTPS in the last quarter of 2020. And if that was not reason enough to worry, hackers are also using legitimate sites that have been compromised to host phishing pages, which makes it even tougher to detect malicious activity.

## Phishing-as-Service

We have heard of software-as-a-service, infrastructure-as-a-service, and platform-as-a-service. Well, make room for phishing-as-a-service (PhaaS).

Now, hackers can subscribe to PhaaS kits on the dark web, ranging in price from about $50/month to around $100/month (USD). There are reportedly over 5,000 PhaaS kits available, and most of them include one or more evasion mechanisms, such as: HTML character encoding, content encryption, inspection blocking, URLs in attachments, content injection, and legitimate cloud hosting (which we look at in the next section). According to cloud internet security provider Cyren, which has conducted in-depth research on PhaaS:

*A straight line can be drawn between the availability of such kits and turn-key phishing platform services and the growth in evasive phishing—phishing attacks that use tactics to confound detection by email security systems. Today's reality is that we are seeing more evasive phishing campaigns in the hands of more attackers at less effort and lower cost than in the past, as technically sophisticated phishing attack developers have adopted a SaaS business model to let even the most amateur criminal wanna-be spoof targeted web sites with a high degree of authenticity and embedded evasive tactics.*

## Hosting Phishing Landing Pages on Public Cloud Services

Businesses are not the entities that are using the cloud to expand their footprint and execute their vision — hackers are using the same innovative playbook to carry out phishing attacks.

For example, in 2020 it came to light that hackers had leveraged the infrastructure of Amazon's and Oracle's public cloud services to host phony landing pages. They then used compromised accounts to target Office 365 users — primarily C-level executives in SMBs — with fake notifications of voice messages and Zoom announcements. Once an unsuspecting user clicked the email link, they were redirected through several proxies, including AWS load balancers, to a legitimate yet compromised website.

And still, the story gets worse: hackers also have the capacity to detect incoming connections from a sandbox environment (an isolated virtual machine in which potentially unsafe software code can execute without affecting local apps or network resources). If detected, the connection is automatically redirected to a legitimate site, and as such, alarm bells do not go off.

## Phishing That Uses Typo-Squatted Domain Names

Another advanced phishing technique uses typo-squatted domain names (also known as a homoglyph attack, script spoofing, and homograph domain name spoofing). Hackers exploit the likeness of character scripts to build and register phony domain names that look very similar to the original, authentic version.

For example, hackers created a phony Adobe.com website that used the Latin small letter b with a dot below (Unicode hex: U+1E05) instead of the normal letter b (hex code: U+0062). In addition, hackers made the site HTTPS (an increasingly popular tactic as discussed earlier). Instead of downloading the Adobe Flash Player installer file, users were served the Beta Bot trojan.

In addition, researchers found that some attacks involving typo-squatted domain names had been injected with an innocuous loader for an icon file. This loaded a copycat version of the favicon from the typo-squatted domain, which ultimately allowed hackers to Javascript skimmer known as Inter.

## Phishing That Uses Inverted Landing Page Backgrounds

A more recent advanced phishing technique involves inverting images that are used as backgrounds for landing pages. Why would hackers do this? Because it is a creative way for landing pages to avoid being detected as suspicious or malicious by various security tools that scan the web for phishing sites. As pointed out by the cybersecurity company WMC Global:

*Because image recognition software is improving and becoming more accurate, this new technique aims to deceive scanning engines by inverting the colors of the image, causing the image hash to differ from the original. This technique can hinder the software's ability to flag this image altogether.*

## Fighting Back Against Phishing

There is no silver bullet that can 100% eliminate phishing. As long as there is digital communication of one kind or another, there will be hackers who will try and exploit these channels to steal private, confidential, and proprietary information.

However, there are some practical and strategic things that organizations can — and given the stakes and impact, should and must — do now to fight back:

- Train employees on how to detect malicious emails. One way to support this goal is by running simulated phishing campaigns — which can yield some surprising (in the disturbing sense) results. For example, in 2020 14% of insurance workers failed a global phishing test.
- Require all employees to choose strong, unique passwords for accounts. Using a reputable password manager is highly recommended.
- Enforce MFA to reduce the risk of account takeover.
- Implement a secure email gateway that automates anti-spam, anti-malware, and policy-based filtering (Note: As discussed above, these tools are not guaranteed to stop all advanced phishing attempts, but they are still an important piece of the puzzle.).
- To increase the capacity to identify and block spam, implement SPF (Sender Policy Framework), DMARC (Domain-Based Message Authentication, Reporting & Conformance), and DKIM (Domain Keys Identified Mail).
- Implement anomaly detection at the network level for inbound and outbound e-mails.

## The Bottom Line

Phishing has evolved dramatically in the last quarter century. Hackers have upped their game because the value of stolen data has never been greater. In fact, top-tier cyber criminals can make around $2 million US a year — which puts them on par with the highest-paid CEOs.

To avoid being victimized, individual users and organizations as a whole need to be educated, vigilant, and equipped with advanced technology. No, this will not completely eliminate phishing. But it will make the lake that hackers phish in much shallower and smaller.