Know the Threats: Examples of Phishing in Cyber Security



ARTICLE 03.22.22 DEAN DORTON

The wave of cyber crime in the world today has swelled into a tsunami.

Individuals, small and large companies — even governments — are under attack by cyber criminals who are constantly evolving traditional threats. They're leveraging the proliferation of remote work environments combined with the expansion of smart devices to lure victims into their phishing scams.

From 2019 to 2020 alone, the FBI reported that nearly 800,000 complaints of cyber crime resulted in more than $4.2 billion in damages. Unfortunately, the expectation is that cyber attacks moving forward will prove that bad actors are capable of making an even bigger splash with illegal phishing expeditions.

Why is phishing so successful for cyber criminals?

Phishing scams have come a long way since the days of an *urgent message* from the "prince" of a foreign country seeking help to transfer funds.

But what today's phishing attempts have in common is that they're still a form of social engineering, targeting the weakest link in the cyber security chain: the human element.

In fact, according to a recent Forbes article, as attackers work to make their phishing attacks more targeted and effective, they've "started researching potential victims, working to collect information that will help them improve the odds that their attacks will succeed."

The truth is, as cyber criminals become more emboldened and less concerned about repercussions, attacks will only grow more viscous and visible. In order to protect yourself and your company, it's important to know why phishing works, and what it looks like.

Phishing examples and why they work

The list and types of phishing scams infecting personal computers and corrupting company networks today is long. And growing at a rapid rate.

In our previous overview of phishing we identified several different types of phishing excursions. Here we'll explore a few examples of each, and some of the reasons they're so successful for cyber criminals.

Phishing emails

It's a scam that's been around since the mid-90s, yet is still surprisingly effective. Phishing emails work because cyber criminals count on the human trust factor — and negligence. As bad actors continue to evolve techniques to closely imitate familiar companies (or even individuals), unsuspecting recipients easily mistake them for legitimate communications.

These messages typically come with a request to take action, often positioned as "urgent." Action requests can include things like **updating a password, clicking an attachment or link** to "important account information," and even responding to a seemingly harmless **social media request.**

Some phishing email examples include:

- **Account deactivation notice:** Online products, services, and storage platforms potentially linked directly to a credit card or bank account are fertile grounds for cyber criminals. In this case, the user receives an email that their account will be deactivated unless they *immediately* confirm or update their login or payment information.
- **Credit card alerts:** With even so much as an indication of a recent purchase, cyber criminals can generate a message to the victim disguised as that company's customer support. From there, customers receive a message that their information may have been compromised — and that protecting their account requires a confirmation of their card details.
- **Request to login or update login information:** These can appear to come from trusted sources like email providers or popular cloud-based services (such as Dropbox, Google Docs, etc). Sophisticated email scams suggest they've updated login credential policies, and encourage victims to click a link to view a document that lands users on a spoof website page nearly identical to the credible site.
- **Fake invoice, purchase, or delivery confirmation:** These continue to be some of the most effective tools in the cyber criminal tool belt. The message notes a pending payment for a phony previous purchase or confirmation for delivery of those goods, relying on urgency and fear to click a link or download the document.
- **IRS notification:** Preying on the fear of repercussion, IRS scams can imply a user is in default of back taxes due immediately. Or that their identity needs to be verified in order to ensure accounts are current and in good standing.
- **Social media message:** Once added to an account as a friend or contact, cyber criminals attempt to lure victims with seemingly harmless invites to view videos or "check out" links that install malware that can crash personal computers or company networks.
- **Organizational tech support:** Bogus messages from a corporate IT department to update or install new software can appear legitimate to the uninformed employee. With minor tweaks to the email sender account, these attacks can lead to network-wide compromise, and the potential for ransomware installation.

Why is email phishing successful?

In addition to relying on human error, cyber criminals have learned to **evade detection** from network email filters by incorporating **legitimate links** sent from reliable sources.

Hackers are also adept at **blending malicious and benign code** together to fool cloud and other online protection software that compromise account credentials. **Redirected** or **shortened links** help cyber criminals fly under the radar with victims, who can also be confused by manipulated brand logos, spoof websites, and the fear of not acting immediately.

Vishing (Voice phishing)

Vishing is the combination of Voice over Internet Protocol (VoIP) with phishing. Similar to phishing emails, these attacks use scare tactics and emotional manipulation to gain access to personal accounts or credentials to breach corporate networks.

In some cases, simply getting the victim to repeat their first and last name can be enough to allow sophisticated criminals opportunities to inflict damage.

A few examples of vishing include:

- **Bank impersonation:** Scammers claiming to be from a financial institution alert the potential victim that there has been unusual or fraudulent activity on their account.
- **Tech support fraud:** An unsolicited call or voicemail that advises anyone to call a number to resolve a problem with a device, program, or online account.
- **Program enrollment or payment scams:** Cyber criminals often prey on the elderly, pretending to work for organizations such as AARP, Medicare, or social security under the guise of helping them collect unclaimed benefits. Or scammers may claim to be with government or collection agencies warning victims about overdue payments and penalties.
- **“You’ve won!” calls:** Whether it’s a cash reward or offer for a prize, recipients are notified of the “limited-time” offer and asked to divulge sensitive data to collect.

Why is vishing successful?

Malicious actors are able to **disguise their number** to make it appear to be a legitimate call from a company or service within the victim’s area code. Or they leave **callback numbers** with urgent requests to return that are difficult for many to resist.

Digital attackers also target company customer representatives or help desks by employing “the mumble technique” in the hopes that their “answer” will suffice. They play on human emotions and willingness of the representative to be helpful — especially to callers who they believe may be impaired — in order to gain useful information to manipulate personal accounts or even company networks.

Smishing (SMS phishing)

Much like email phishing, smishing attacks target unsuspecting recipients with malicious short links **via text message**. While this technique is nothing new, the fact that 96% of Americans now own cell phones (81% smartphones) means smishing continues to gain traction with cyber criminals.

As with phishing emails and vishing calls, examples of smishing include:

- Urgent messages about credit cards
- A locked or compromised bank account
- Government or collection agency scam

Perhaps **the most common smishing attack** these days attempts to come from a trusted consumer brand such as Amazon, FedEx, or UPS, with a link to track a package. With millions of packages delivered daily, cyber criminals play the odds and assume someone will click and divulge sensitive personal information to receive their shipment.

Why is smishing successful?

People are accustomed to immediate access to emails, phone calls, and text messages. With a simple click, smishing attempts can trigger the automatic download of malicious apps on mobile devices that can deploy ransomware or enable cyber criminals to remotely control devices.

This can be especially devastating for organizations with remote employees who may be careless with their personal devices that are connected to company networks.

Spear phishing

While email phishing favors the quantity of victims targeted, spear phishing is all about quality. It’s a more involved and evolved type of cyber attack that allows the attacker to create a customized scam featuring insider information of that individual or company.

Examples of spear phishing include:

- **CEO fraud:** Cyber criminals pose as C-suite executives aimed at the highest levels to request or glean important details.
- **System admin attack:** As an example, an email is delivered to a system administrator from what appears to be a credible IT provider offering a new or free service. Once clicked, the admin is redirected to a phony page where a command and control agent can access the network.

Why is spear phishing successful?

The targeted nature of spear phishing attacks make them difficult to detect. Digital attackers are increasingly housing malicious documents on trusted cloud-based services like Dropbox, Box, Google Drive, and others. Therefore, IT departments responsible for the email filters may not allow them to flag the corrupted files.

Cyber criminals can also gain access to information about higher level execs at a targeted company by seeking employees on social media to investigate the organization's structure.

Session hijacking

Also known as cookie hijacking, attackers overcome the target's computer session and then act as that user without having to provide authentication.

Examples of session hijacking include:

- **Cross-site scripting:** Cyber criminals inject scripts that capture session tokens, tricking users into clicking a malicious link to a known website that requests authentication.
- **Session sniffing:** A more active type of hijacking attack, here bad actors "sniff" for unencrypted network traffic for session cookies to use masquerading as the victim.
- **Session fixation:** In this type of attack, cyber criminals can set a user's session ID to assume the role of the intended user.
- **Brute force:** Hackers simply guess and determine the session ID. Prime targets are the business systems that create session IDs based on time, date, or the user's IP address.

Why is session hijacking successful?

When cyber attackers are able to assume a known user's identity, they gain all the same authentications and certifications as the compromised user. As far as the server knows, the attacker is the authenticated source and no longer has to provide additional credentials.

Malvertising

Difficult to detect by users and hosts of sites, malvertising is a type of phishing attack where a third-party server is breached without the user's knowledge. These are often determined by a user's browsing habits and clicks.

There are several known forms of malvertising, including:

- **Content or text-based:** Malicious codes get added to simple text-based advertisements on host websites, typically in the sidebars or in the main content body.
- **Banner ads:** Attackers lure website visitors into clicking an ad which can display fake deals or coupon codes, including (ironically) virus infection-protection related messages.
- **Video ads:** Malware-laden videos that look like legitimate ads for product or services ads, or feature clips of video games, breaking news, and celebrity interviews.
- **Animated ads:** Attackers insert malicious codes into Java scripts or Flash player.
- **Inline frames:** One of the HTML features that developers use to create content. Attackers exploit the i-frame by keeping its dimensions set to 0x0 pixels. While website visitors can't see any content, the host website still carries it, automatically downloading malware after visitors spend just a few seconds on the site or click on the infected message.

- **Pop-up ads:** Attackers use popups to deploy malware, with the bait being things like a survey, poll, coupon codes, deals for a limited period of time, free products, or free subscriptions.

Why is malvertising successful?

Malvertising is one of the most effective forms of phishing because it preys on our gullibility. What's more, the sheer **volume of digital ads** served daily is staggering, making it difficult for legitimate sites to verify. And because malvertising attacks require the user to interact with the infected ad, not every visitor will be affected. This makes it more difficult for cyber security to narrow down the dangerous content.

Pharming

Pharming attacks are similar to phishing emails in that both trick users into divulging private information. But in a pharming attack, email messages are not necessary. Cyber attackers install malicious code on a computer or server that can be used to send victims to a bogus website.

Examples of pharming include:

- **Malware-based:** Sent in an email or in a download, corrupted files can direct a computer to fraudulent sites regardless of the intended address.
- **DNS server poisoning:** A corrupted DNS server can direct network traffic with potentially millions of users to an alternate, fake IP address.

Why is pharming successful for hackers?

Besides the initial execution of the malware, the user doesn't have to click anything they may see as suspicious. Once the malware is installed and is executed, it remains on the computer — even after it's been rebooted. Only malware removal tools can delete files used to monitor user activity, show popups, or hijack browser settings.

Whaling

Often launched via emails, whaling targets CEOs, C-suite, and other upper level executives of an organization. After all, they are keepers of some of the most sensitive information, and makers of the biggest big decisions. A compromised executive's account is more effective than a spoofed email account, and can lead to ongoing attacks to that company or other organizations in the supply chain.

Techniques for whaling may vary from **emails, to phony invoices**, to **vishing** or **smishing**. But the end goal is always the same: to acquire sensitive information for financial gain or corporate compromise.

Why is whaling successful for hackers?

Upper-level executives are typically the most busy, stressed, and overworked. Under duress, people are prone to make mistakes.

Real world examples of phishing

Phishing of any type can cause financial loss, grant cyber criminals access to information used to commit crimes against others, or damage a company's reputation beyond repair. Here are a few examples of "successful" phishing expeditions, and the cost it levied on victims.

Iowa Company loses $265,000 in business email scam

An employee at an Iowa company received an outstanding invoice email in May of 2019 that appeared to be from their contact at a legitimate Texas company they did business with.

The email informed that the Texas company's banking information had changed, requesting the Iowa company update its bank records. That led to two illegal wire transfers totaling more than $265,000.

Vishing attack on Geek Squad

In June, 2021 Geek Squad customers received an email requesting they contact a bogus phone number to suspend supposedly fraudulent subscriptions. The email bypassed controls and infected 25,000 inboxes.

FedEx smishing attack

Following the 2019 Christmas rush, millions of people began receiving text messages claiming to be from this shipping giant. The alert encouraged victims to set their "delivery preferences." Anyone who clicked the link were directed to a fake Amazon customer satisfaction survey that offered a free gift as a reward — IF they entered their credit card details to pay for shipping.

Compromised password costs Colonial Pipeline $4.4 million

Ransomware attackers gained access to Colonial Pipeline computer networks in April of 2021 using a compromised password. It had been linked to a virtual private networking account used for remote access, and was not guarded by multi-factor authentication. In order to restore services, Colonial CEO Joseph Blount authorized the mega payout.

Session hijacking costs Crypto.com nearly $35 million

In January, 2022 cyber criminals infiltrated the accounts of 483 accounts by slipping past two-factor authentication. The attack drained accounts, forcing the company to reimburse the losses.

Defending against phishing attacks

Keeping your cyber security guard up is the best, most effective first step to take. Assume your organization's network is vulnerable — even consider that cyber criminals have you in their sights. From there, general, preventative measures such as employee training, constant network monitoring, and consistent communication throughout the organization can help not only mitigate risk, but put a plan in place to quickly and efficiently recover from a phishing cyber attack.

The threat of phishing attacks are real, and require ongoing vigilance and attention. Safeguard your critical information — and your reputation. Connect with Dean Dorton for a cyber security risk assessment or audit today.

And for more insights and analysis on trends and cyber security solutions, be sure to subscribe to our blog.