ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Unfortunately, Phishing is Still in Season

Technology, Privacy, and eCommerce

According to ACC surveys, phishing risks and countermeasures are a top concern for in-house counsel. And the problem isn't going away — in fact, the scope of the problem is increasing in the chaotic COVID-19 world.

Each year, Verizon publishes its *Data Breach Investigations Report*, one of the most comprehensive such reports — and one I highly recommend. According to the 2020 report, phishing incidents accounted for 22 percent of all breaches.

So, what is phishing anyway? Phishing is when hackers pose as a trustworthy counterparty in an electronic communication, including phone calls. The hackers use trickery (so-called "social engineering") to fraudulently obtain sensitive or other valuable information (like usernames, passwords, or credit card details), or to install malware on devices.

Many people first became aware of phishing scams in the early 2000s, when the so-called "419" Nigerian email scams were prevalent. The scams conned gullible targets out of savings through emails from purported Nigerian officials or royalty. These email frauds offered their targets the "opportunity" to share in a percentage of "millions of dollars" that these Nigerians supposedly needed help transferring out of the country, allegedly to avoid other corrupt Nigerian officials and return the funds to their "rightful owners." Targets were tricked into sending confidential information to the "officials," such as bank names and account numbers, and into paying for certain facilitation expenses. Needless to say, these didn't end well for their victims, who were collectively conned out of millions and millions of dollars.

Those early email scams were easily recognizable as fishy because they were written in broken English and requested information in unconvincing ways. But like everything else in technology, that has dramatically changed. In the intervening years, phishing has become so sophisticated that even intelligent and knowledgeable people have difficulty recognizing them.

The COVID-19 pandemic has only made this situation worse. For one thing, some of the protections we may have had while working on-premise may no longer be in place while we are working from home. Disasters also provide fertile soil for phishing because people are distracted, often overlooking details, especially when they are motivated to help the less fortunate. Right now, for example, some phishers posing as the CDC or WHO, or as hurricane or wildfire relief organizations. The people behind these things are as unscrupulous as they come.

As mentioned, phishing may impact you even if you don't directly fall prey to a phishing attack. If someone hacks into one of your trusted websites by using phishing techniques, like the Target hack affecting 110 million users in which a third-party vendor was tricked into granting the hackers access, your personal information may be exposed. This is bad enough if it involves things like credit card numbers, but it can become even worse if it turns out that the hackers have gained access to other sites or accounts such as your email. They will then leverage that information to steal more of your money or attack other victims by posing as you. In the Equifax breach, for example, many people were tricked into giving the hackers additional information that enabled access bank and other accounts.

Massive amounts of stolen records are bought and sold on the dark web. These are then cross-referenced and merged with personal or corporate information from previous breaches to create incredibly sophisticated, tailored phishing attacks, not only against individuals but corporations as well. Notable data theft events from Equifax and EDGAR have made it easier for criminals to launch targeted phishing campaigns against high-value organizations. So, for example, information obtained from a trading partner may be used to generate false invoices that appear genuine. Or, phishing could be used to steal confidential customer information that could create tremendous liability for your company. Remember, phishing is not just a personal risk — as corporate lawyers, it is important to be aware of the issue so you can help try to minimize those risk to your organization.

Here are some kinds of phishing attacks and tips that may help.

- While email is still the biggest vector for phishing attacks, other vectors are becoming increasingly popular among criminals. Phone call phishing attacks (aka vishing) are becoming more prevalent and sophisticated. A few years ago, vishers used robotic voice calls pretending to leave messages from the IRS and similar things. My mother-in-law once received a call from a purported EMT worker claiming that her granddaughter had been in a car accident and her credit card info was needed to pay for her “care costs.”

Scams like those have become easier to spot, but these days one of your IT employees might receive a call claiming to be from your specific IT vendor or from a specific company employee having trouble accessing your company VPN, with just enough plausible detail to convince them to give them access information. These vishers even have devices that can get through your company’s two-step verification process.

The best advice for the current environment is to educate employees to systematically verify such calls by hanging up and dialing a known contact number for that vendor or employee to ensure their validity.

- SMS message phishing (smishing) has also become a popular vector. You may have received texts from strangers asking you to take part in a survey, political poll, or product offering, along with a link. Those may or may not have been legit. I recommend deleting any of these unless you actually know the sender. And if you want to be even more cautious, consider contacting any known sources where the link may seem out of character to make sure the message really originates from them.
- With our mobile devices quickly becoming the most widely used computers in the world, it is no surprise that hackers try to trick users into providing access to them. One way for them to do this is to trick users into installing unsafe apps. Android and iOS devices have built-in hardware and software security protections to make this more difficult, and app store review processes can help identify and reject malware apps (although some do manage to creep through, especially on Android). More importantly, phishers will try to trick users into downloading “apps” from sites that appear to be legitimate app stores but aren’t.

For example, in order to help bypass security protections offered to Android users by the Google Play Store, cybercriminals have used comments below YouTube videos or links in popular chat apps that claim to offer free or cracked versions of well-known Android applications. The download pages for these fake applications use the same icons, text, and imagery as the real app, to add authenticity and encourage potential victims to download the malicious software. Then the app will seemingly disappear after installation by disguising itself as something under the settings menu of the phone. Or the app will claim that it can’t be installed in the user’s country — while secretly installing the malware.

My advice is never to download apps except from the app store on your device. And if something suspicious does happen and your device starts acting more oddly than usual, you may want to wipe and restore it from a backup. (You do keep backups, I hope.)

- Social media has also become a dangerous phishing vector.
    - In 2016, thousands of Facebook users received messages telling them they’d been mentioned in a post. When they clicked the link, it initiated a two-stage attack. The first stage downloaded a Trojan containing a malicious Chrome browser extension onto the user’s computer. When the user next logged into Facebook using the compromised browser, the criminal was able to hijack the user’s account, enabling

them to change privacy settings, steal data, and spread the infection through the victim's Facebook friends.
    - The notorious Twitter breach in July that compromised more than 130 accounts belonging to celebrities and other public figures was the result of a "phishing" scam in which hackers used the phone to fool Twitter's employees into giving them access. The attack affected the accounts of some of Twitter's most high-profile users, including Tesla CEO Elon Musk and celebrities Kanye West and his wife Kim Kardashian West, in an apparent attempt to lure their followers into sending money to an anonymous Bitcoin account.

This not only points out the dangers of social media, where it has become increasingly easy to spoof particular users, but also the importance of training company employees so they are not so easily tricked.

Phishing is a pervasive and persistent threat. This article has barely touched on just some of the risks and precautions. I plan to write more about this in the months to come.

References

Microsoft Corp. customers were targeted in a phishing campaign that has sought to defraud users in 62 countries since December. Recently, the malicious emails have evolved to capitalize on the pandemic, by using attachment names related to the pandemic, such as "COVID-19 Bonus." Coronavirus-themed phishing attacks have become so pervasive in recent months that the US and UK governments warned about their growing use. For example, in March, the number of attempted phishing emails sent by criminals and state-linked actors more than quadrupled amid the spreading virus, the cybersecurity firm FireEye Inc. reported. A Sebenius, **Vast Phishing Campaign Hits Microsoft Users** in 62 Countries, July 7, 2020, https://www.bloomberg.com/news/articles/2020-07-07/vast-phishing-campaign-hits-microsoft-users-in-62-countries

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant