Recognising and preventing modern cyber scams

By Doros Hadjizenonos

22 Oct 2018

When it comes to protecting yourself and your organisation against cyber scams, there's no "one-size-fits-all" solution. As organisations and people alike continue to adopt new devices and technology, they're opening themselves up to more opportunities for cyber attacks.

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

In order to effectively protect the valuable information that motivates cybercriminals, it’s important that we understand the different types of scams targeting us.

Understanding the warning signs of modern cyber scams

Cybercriminals use a wide variety of scam tactics in order to gain access to a device or network, extort money, or steal valuable information. When it comes to understanding today’s threats and how to protect yourself and your organisation against them, knowing the various ways they leverage social engineering tactics to trick users can go a long way.

With this in mind, people can minimize the impact of cyber scams by learning about common variations being used to

target them:

1. Phishing scams

Phishing attacks are an all-too-common occurrence in both corporate and personal networks. They happen when a criminal sends a communication (email, phone call, text, etc.) pretending to be someone else in order to extract or access credentials, personal data, or financial information about the targeted individual, or sensitive information related to the organisation for which the target works.

What's more, according to IBM research, 59% of all successful ransomware infections are transported via phishing scams.

Here are a few things to be aware of to help you better recognise these malicious scams:

- **Check contact names**: Use caution if you receive communications from a source you don't recognise that asks you to take an action, like providing personal information or signing into a site. Most, if not all, companies will never prompt you for your information via email or text. When someone does, this should be considered a red flag that they're not who they say they are. Check their email address or phone number and compare it with the person or organization they claim to be associated with for inconsistencies.

- **Look for misspellings and poor grammar**: Professional organisations take the time to read their communications over before sending. Oftentimes, phishing cybercriminals do not. If you receive a message from a supposedly trusted source that includes typos, poor grammar, or bad punctuation, chances are it's a scam.

- **Look for aggressive behaviour**: If the subject matter and language of a message is overly aggressive, it is likely a scam. Have you ever seen an email in your SPAM folder saying something similar to, "Urgent! Your account is X days overdrawn Contact us IMMEDIATELY"? The goal here is to make you uneasy, panic, and take the action the scammers want. Instead, check with the party they claim to represent before taking any immediate action.

2. Spear phishing scams

While phishing attacks are sent in mass and offer relatively easy-to-spot clues, spear phishing is its highly targeted and much more sophisticated counterpart. Spear phishing scammers conduct in-depth research about their victims and take the time to understand their organisation, colleagues, interests, etc. in order to boost their chances of success.

To better protect yourself from spear phishing, consider the following:

- **Use an email verification service**: Email verification works by validating the source of the emails you receive to check whether or not the identities of the Administrative Management Domain (ADMD) match the email address being used.

- **Use discretion when handing over information**: While it sounds simple, if users weren't willingly handing out their information to bad actors, phishing wouldn't be an effective scam.

- **Maintain good security hygiene**: When you practice basic security hygiene, you deny scammers many of the common attack vectors they use to infect your machines and gain access to your information or organization's network. The implementation of simple, everyday habits can go a long way toward preventing scams from successfully compromising a device or network.

3. Baiting scams

Baiting scams, as the name suggests, aim to bait unsuspecting users into performing a certain action like downloading a virus or entering personal information in exchange for the "bait." This bait can be anything from free anti-virus software or movies users can download, to physical bait such as a thumb drive labelled, "Corporate Salary Information" left out for a victim to find and plug into their machine. While this type of scam can take many forms, the end goal is always the same: luring users to install something malicious.

To protect yourself and your organisation, pay attention to these common indicators:

- **Avoid "free" deals**: As the old adage goes, "If it sounds too good to be true, chances are it is." Many cyber scammers will attempt to lure victims in with promises of free downloads, free shipping, free subscriptions, etc. So, be sure to not only double check the source and read the fine print of any agreements, but also do some checking on the organisation claiming to make these offers.

- **Avoid unfamiliar external flash drives or hard drives**: Baiting can be done digitally or with physical drives that install malicious software. Make sure you know the owner of the drive before you connect it to your machine.

4. Tech support scams

In 2017 alone, the FBI reportedly received around 11,000 reported cases of tech support fraud, costing a staggering total of $15m in damages. As the name suggests, scammers will pose as tech support employees, either working for a victim's organisation or for an independent service, in order to gain access to personal information. Like the other scams listed here, success or failure is dependent on the victim falling for a social engineering attack.

With this in mind, it's important to watch out for some of the telltale red flags:

- **Lookout for unsolicited messaging**: Rarely, if ever, will tech support reach out to "check in" or offer to fix your computer. Software and hardware developers never track their solutions and then call to offer security assistance. If a tech support worker or company is reaching out to you via a popup ad, and unsolicited email or phone call, or through social media, it is likely a scam. Legitimate companies have established processes in place to update your products and services, such as published patches and updates, or ways to address issues that are built directly into the solution itself.

- **Avoid installing anything from an unknown source**: Unless it comes directly from a source you trust, downloading anything from the web comes with the inherent risk of infecting your machine. Like baiting scams, cybercriminals will often attempt to offer "free security scans" or "computer clean-ups," which then infect the victim's computer with malware.

- **Lookout for actors who want remote access to your device**: Remote access allows real tech support teams to "take over" a machine remotely in order to fix it. However, the same technology can be used to quickly access personal information off of your device. If a source you're unfamiliar with asks to gain access to your device, steer clear.

5. Securing mobile devices

Mobile devices are also being increasingly targeted by criminal scams. Fake applications used to mine for data or ransomware are widely available, especially for Android operating systems.

- **Avoid malware masquerading as legitimate applications and updates**: A growing number of fake applications are available from third-party app stores (e.g. Apkmonk). In addition, implants and updates that exploit applications and devices also abound (such as cryptojacking malware). Also be wary of apps requesting unneeded permissions (e.g. Device Admin

and SMS exploits, etc.)

Cryptojacking - a silent threat

11 Sep 2018

- **Use secure WiFi**: Be mindful of free WiFi. Public spaces and shops offering free Wi-Fi connections are common locations for man-in-the-middle attacks where criminals will often broadcast the availability of Wi-Fi services and then use them to capture data. When using public Wi-Fi, use VPN connections and avoid sensitive transactions. Many mobile apps are also programmed to automatically connect to known connections, so cybercriminals often use common Wi-Fi SSIDs, such as “Home Network” to trick devices into automatically connecting without requiring any user input.

Data breaches compromised 4.5 billion records

11 Oct 2018

6. IoT devices

Iot devices are also an increasingly popular attack vector. Many IoT devices are easy to exploit, have a persistent internet connection, and use powerful GPU processors, making them ideal for crypto mining and DDoS exploits.

- **Update credentials**: The most common exploit strategy is to simply attempt to connect to an IoT device using its default username and password. Whenever possible, change the password on your routers, smart TVs, and home entertainment systems, etc.

- **Connected cars**: As more and more devices become interconnected, they become vulnerable to the weakest link in the chain. Devices like connected cars are not only rich targets for attackers, containing user data, phone contact information, and even payment information, compromise can also pose a risk to drivers and passengers. When purchasing a connected car, carefully review and change its default security settings and avoid app installs from unknown sources. In addition, review the security and credentials of Bluetooth connected devices, especially those that interface with your car’s network.

Final thoughts

Cyber scams can affect anybody unaware of these common warning signs. As people continue to adopt more and more devices that connect to a network, the risk of falling victim to a scam only increases. By being aware of the common cyber scams targeting people today, as well as recognising the telltale signs of those scams, you can safeguard your valuable information and the information of the networks you connect to.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...