November 2020

BRIDGE
ADVISORY

Cybercriminals Exploitation of Stay-at-Home Orders

Most of us can agree that during these countless months under stay-at-home orders, life has taken on a peculiar image -- and we may have developed severe shopping addictions. Although, whether it be shopping, banking or even socializing, consumers have had to move almost all aspects of our lives onto the internet. And just like in the physical world, there are criminals amongst us. Cybercriminals are taking advantage of this dramatic shift and becoming increasingly aggressive online, actively exploiting our new norm. Not only are these attacks happening to consumers on a personal level, but corporations have been targets as well.

> “Tom Kellerman, head of cybersecurity strategy at VMware Inc., testified before the House Subcommittee on National Security, International Development and Monetary Policy late last month, saying that cyber-attacks against the financial sector rose by 238% between February and April, the peak period when COVID-19 was spreading across much of the U.S., forcing government imposed stay-at-home orders.[1]”

These attacks can come in many different forms and some may look very real, claiming to be from respected organizations. Unfortunately, some of these organizations have been hacked as well. The World Health Organization (WHO) reported a significant increase in the number of cyber-attacks directed at its staff which resulted in over “450 WHO email addresses and passwords” that were leaked online and then used to target the public to make donations to a fake WHO account to fight the pandemic. (W.H.O., 2020) Scammers are also contacting the public impersonating local COVID tracers and asking people for their public information.

So how do we protect ourselves from cybercriminals? Do not fret, these are not the same type of “hackers” you see in the movies, they cannot just access your information at the flip of the switch or a few keyboard entries. We must, however, educate and prepare ourselves for these attacks. This includes acknowledging that our new home offices are more vulnerable to the sophistication of phishing* techniques. Working from home usually means that we are using personal devices that may be older or not up to date with cybersecurity software such as antivirus or VPN’s. Meanwhile in most office environments, IT managers generally control the cybersecurity of all devices and Wi-Fi networks.

Some basic procedures we can all take to better protect ourselves include:

- Avoiding public Wi-Fi - unless using a VPN* service on your device.
- Updating your Wi-Fi password on a regular basis, keep the current password on a note within your home and never on another device.
- Equip all devices with active firewalls and protective software.
- When accessing sensitive information, ensure you are using a VPN.
- Using two-factor authentication wherever possible - typically requires a security code be sent to your smartphone or email to complete access.

Now keep in mind, even the most advanced security software cannot protect us from all the different forms of phishing and data breaches. About 90% of data breaches are the result of human error.[2]

Phishing

OK so "phishing" is bad, but what the heck does it mean? Phishing is the practice of sending fraudulent communications that appear to come from a reputable source such as a friend (whose email has been hacked), government agency or a popular company. These scam messages are usually received via email or a pop up that prompts you to click a link or request your phone number so the scammer can contact you.

Once successful in gaining access, malicious software (also known as malware) allows cybercriminals to take complete control of your computer, granting them access to personal and financial information by utilizing saved passwords to your online accounts. The sole purpose of phishing is to con the victim into revealing private and confidential information. We are all distracted at home with kids, work, errands, etc. and are more likely to click links without further inspection.

> *"The extent of this new phishing threat is huge. Google's Threat Analysis Group reported in mid-April that they blocked 18 million COVID-19 themed malware and phishing emails per day." (Spadafora, 2019)*

A newer method in which cybercriminals are exploiting this work-from-home period is through fake Zoom or other video conference invites that allude to possible layoffs or crucial conversations that need to be had. This new phishing campaign aims to trick people into thinking they have a potential meeting with HR or someone higher up in the company that must join. These invites will use certain words such as *payroll, crucial, All Staff Meeting or Termination.* These words are meant to cause instant panic so that the victim quickly clicks the link to join the fake meeting. Make sure to avoid emails, calls or pop up messages that insist you act now or demand immediate action. Most certainly make sure to **never give personal information when someone else has initiated the contact.**

> “Click it and you’ll be taken to a website with a login window that looks very much like Zoom’s. A quick inspection of your browser’s address bar will reveal that you’re not actually on the Zoom.us website.” (Mathews, 2020)

In an emergency, worst case scenario, these are some crucial steps to take:

1. If the cybercriminal has already accessed your computer, immediately disconnect your device from the internet. This can mean unplugging the device itself, or even unplugging the router in your home.
2. File a complaint with your local law enforcement or the FBI’s Internet Crime Complaint Center (IC3) - https://www.ic3.gov/default.aspx
3. Inform all necessary contacts -- Credit card companies, banks, financial advisors, CPA’s, colleagues, family and friends.
4. Update all passwords, especially your Wi-Fi, email and financial accounts. Make sure to keep these passwords off any devices, the best way is actually the old-fashioned way - in a password notepad or notebook in your home.
5. Continuously monitor your accounts.

This may all seem extremely intimidating and frightening at first, but with this knowledge and newfound vigilance, spotting phishing scams will become much easier.

Jones, D. (2020, June 19). COVID-19 pandemic caused increase in cyber fraud and changes in banking. Retrieved from https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2/

W.H.O. (2020, April 23). WHO reports fivefold increase in cyber attacks, urges vigilance. Retrieved October 22, 2020, from https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Spadafora, A. (2019, May 08). 90 percent of data breaches are caused by human error. Retrieved from https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error

Mathews, L. (2020, April 28). New Phishing Attacks Prey On Job Loss Fears With Fake Zoom Meeting Invites. Retrieved from https://www.forbes.com/sites/leemathews/2020/04/28/new-phishing-attacks-prey-on-job-loss-fears-with-fake-zoom-meeting-invites/