In this issue:

- **Hack-Proof your remote office setup**
- **Emerging COVID-19 cybersecurity threats**
- **Cybersecurity shorts**
- **Software updates**

Welcome to your March Cybersecurity newsletter. As COVID-19 continues to spread across the world, we are also starting to see cybersecurity side effects. We'll discuss those in this month's newsletter, focusing on topics like how to work from home securely and scams to be on the lookout for. We wish you all good health during these challenging times.

This month saw lots of cybersecurity happenings such as:

- How hackers are using the Coronavirus to spread malware
- Details on a cyberattack at the Department of Health and Human Services
- A hack that may have exposed your images without your knowledge
- And more

Hack-Proof your remote office setup

As COVID-19 continues to spread across the globe, many people find themselves working from home for the first time. While there are many things to get used to when adjusting to remote work, ensuring that your setup is secure should be a top priority. If you are a business owner, you must give your employees resources and information on how they can do their jobs from home while keeping data and networks safe.

1. Make sure connections are secure

As employees connect from home to handle sensitive work documents, you must ensure that everyone is connected to the Internet securely. All businesses should have employees connecting to a virtual private network (VPN) during the workday.

A VPN creates a secure, encrypted Internet connection to connect your device to your company's network. While connected to your regular Wi-Fi, it creates a secure tunnel between a device and the network. This makes it more difficult for hackers to infiltrate your system. Without a VPN, hackers could access your network through insecure employee Wi-Fi.

There are many different VPNs to choose from—some are paid and some are free. We recommend choosing a paid option in these cases. You can review some of the more popular VPN services here.

You should also be sure that Wi-Fi is password-protected with a strong password.

2. Keep software updated

Another thing employees must do when working remotely is to keep their devices up-to-date. That means updating all software on devices including operating systems, Microsoft Office programs, browsers, and more. If you are a business owner, share information on the importance of updating software with employees during this time and give them instructions on how to do so.

Keeping software up to date closes security vulnerabilities hackers can attack to get into your network. If your employees are using their own devices to work from home, you should also inquire about the antivirus software they are using. If they do not have antivirus, you should consider purchasing a program for them.

3. Protect accounts

Using strong passwords and two-factor authentication is always best practice, but especially during these times of widespread remote work. As hackers move to take advantage of an influx of people working remotely, everyone should be protecting online accounts with extra security.

If you don't already use a password manager, now is a good time to consider starting. A password manager is a protected vault to store all of your passwords. Instead of needing to remember thousands of passwords, you only need to remember a Master Password to open the vault. This technology cuts down on people using the same password for multiple accounts.

Employees should be using two-factor authentication wherever possible as well. Two-factor authentication offers an additional layer of security to your account because it requires something you know (your password) and something you have (your device). When two-factor authentication is enabled, you will be required to enter a one-time code after your password. This code is sent to your phone via text message or authenticator app. Even if a hacker has your password, they would not be able to log into your account without the code.

4. Beware of scams

Unfortunately hackers have not let up on scams during this global pandemic. In some cases, they are even using the virus to spread malware. It is important to be especially aware of phishing scams during these times. Many organizations are reporting that hackers are sending phishing emails pretending to be the World Health Organization or others with checklists and information on COVID-19 prep. Review how to handle these emails here and remember to not open emails from outside your organization on this topic.

Emerging COVID-19 cybersecurity threats

The Department of Health and Human Services (HHS) was hit with a cyberattack early in the COVID-19 pandemic. Hackers hit the HHS servers with millions of hits over several hours to try to overload the system. The government says that no one was able to access any networks. The attack is believed to have been carried out by a foreign state.

Hackers use Coronavirus global infection map to spread malware. Security expert Brian Krebs reported on the scam this month. He explains that hackers are taking the legitimate John Hopkins University map tracking the spread of COVID-19 and loading it on to malicious websites. When users visit the sites, malware is installed on their machines. When looking for information on this pandemic, always verify that you are using a legitimate source.

Phishing messages disguised as COVID-19 information make the rounds. Hackers have been sending emails appearing to be from organizations such as the WHO with malicious files disguised as helpful attachments or links. Review our alert from earlier this month.

Cybersecurity shorts

Tax phishing emails continue to hit people's inboxes. The latest one informs taxpayers that they are a non-resident alien must fill out a W-8BEN form. The email includes a fake form that phishers hope recipients will fill out to gather their tax and bank information. Remember that the IRS will not contact you on matters like this via email. If you receive an email like this, delete it.

American consumers and businesses lost nearly $3.5 billion in cybersecurity crimes in 2019, according to a new FBI report. There were about 500,000 complaints reported to the FBI last year—100,000 more than in 2018. Of the billions lost, the FBI was successful in helping victims recover about $300 million. Of the total $3.5 billion, about $1.7 billion was lost to business email compromise scams.

A facial recognition startup, Clearview AI, has exposed photos of billions of people to hackers. According to the company, an unauthorized user was able to access its customer list through a security flaw. That flaw has now been patched. Clearview AI is used by law enforcement agencies and banks. It has over 3 billion photos that it has scraped from websites like Facebook, YouTube, Instagram, and Twitter. The company has been banned in some states.

Democratic National Committee (DNC) warns campaigns of hacking attempts. According to the DNC, an online impersonator of a DNC staffer contacted Senator Bernie Sanders' campaign. These messages often encourage the recipient to install a malicious file or click on a fraudulent link. The DNC is warning all campaigns to be aware of these threats.

Phishing email costs home-searching couple $775,000. A California couple was ready to close on their dream home. They received an email that appeared to come from their real estate agent with escrow instructions and how to wire money. But the email came from a hacker who spoofed the email address to look like the real estate agent's address. Over $700,000 was sent to the hacker. The couple has not been able to recover the money.

Celebrities, too, are victims of common scams. This month "Shark Tank" star Barbara Corcoran lost $400,000 through a business email compromise scam. Corcoran's bookkeeper received an invoice she thought to be from her assistant--but it was really from a hacker. The bookkeeper was savvy and questioned the invoice but the response from the hacker seemed legitimate, so she paid the bill. They later discovered the fraud and are working on getting the money back.

The 2020 Census goes live—online. While many security experts voiced concern over the risks associated with the online Census, households across the country can now complete the census questionnaire online. Due to security concerns, the Census Bureau has printed enough paper forms for

every household in the country. The Bureau switched to new software to collect data after the planned software was not sufficient. Experts worry this new software has not been properly vetted.

If you get your prescriptions filled at Walgreens, your information may have been exposed. The pharmacy chain announced a breach this month. Users of the Walgreens app may have been able to see prescriptions and personal information of other customers. Walgreens says only a small percentage of customers was affected.

Patients soon will have more control over their health data due to new rules introduced by the Department of Health and Human Services (HSS). The first rule would require that health providers give patients access to their health records electronically for free. The rule would also ensure that health providers are storing and sharing this information securely. Any third-party software used would need to be vetted properly.

Software updates

Microsoft: Microsoft released updates for over 100 security issues this month affecting Windows operating systems, Microsoft Word, Microsoft Outlook and more. Many of these flaws are designated as critical and you should update your system as soon as possible. You can learn more about the updates here.