Recommendations for Cybersecurity for Remote Workers During Coronavirus

The rapidly changing situation of potential school closures, self-quarantines, and public reaction to the coronavirus guarantees that at some point you will have employees who need to work from home.

If the employee's computer isn't secure, your organization's security is at risk. Attackers can compromise a home user's device to gain a pathway into your organization's network and data. Whether the attacker installs ransomware, steals sensitive information, or shuts down your entire network, you can suffer greatly. Therefore, you need to take essential steps to protect yourself, your employees, and your organization. Here are some key suggestions to help you navigate this crisis.

Remote Access Tools:

Your employees need to securely access email messages, applications, and data. You may need them to participate in secure meetings. They may need a phone that behaves as a secure extension as if they were at the office.

If you already remote workers, your main concern will be to ensure your servers are powerful enough, your connections to the Internet fast enough, and that you have enough licenses to support the increased volume of activity.

There are so many choices of platforms and tools. Each has its own cybersecurity concerns. You might hear about remote access solutions such as Citrix, GoToMyPC, LogMeIn, Remote Desktop, Splashtop, Terminal Server, and VNC. For meetings you may use BlueJeans, GoToMeeting, Join.me, Microsoft Teams, Skype, and Zoom.* There are others too. Let your IT team use the one they are most familiar with so they can deploy and troubleshoot solutions much quicker. You might ask them to share the pros, cons, and expenses of different solutions, but act as quickly as your risk appetite allows. It is difficult to predict how quickly the reaction to the coronavirus will accelerate.

A VPN Is Not Enough:

There is a worldwide misconception that VPNs provide security. By themselves, they do not. What VPNs do provide is privacy. Think of them as a tunnel that protects data from observation, deletion, and modification while the data travels inside the tunnel. But attacks can lurk at both ends of the tunnel. Therefore, both sides of the VPN connection must be secure. VPNs are useful to protect privacy, and there are other ways to help ensure privacy too.

Connections to the Internet:
Your remote workers need secure connections to the Internet. When they are working from home, they may share their network with less secure family members or compromised IoT devices. That's why connecting at home might be too risky. Connecting to a coffee shop, hotel, or another public place is reckless unless you mandate compensating controls.

Sometimes the best way to resolve many security risks associated with the remote computer's connectivity to the Internet is to provide them with a mobile hot spot. All the major phone carriers provide hotspots and most smartphones have the capability of behaving as a hotspot, enabling employees to connect via mobile phone data plans. Beware that even unlimited data plans are limited; once the user goes over a certain amount of data, the phone provider can throttle the speed of the data to an unacceptably slow connection. If you need unlimited data without throttling, consider a solution such as calyxinstitute.org.* Bear in mind that as more people work from home during the outbreak, mobile data speeds may deteriorate due to congestion. Evening and late nights will usually be faster, not only due to a drop in demand, but also mobile phone providers often allocate more bandwidth to data at night and reallocate bandwidth back to voice calls during the daytime.

Home Wireless Networks:
These days, it's common that your users already have long wireless passwords and use at least WPA2 encryption on their Wi-Fi network. Disable a feature called WPS. WPS is designed to make it easy for people to connect new devices. Unfortunately, it also makes it easier for attackers to connect. If the user needs WPS to connect a new device, they can enable WPS temporarily. There is an option called MAC filtering that permits your user to specify what devices are allowed to connect to the access point so that, in theory, no unauthorized devices can connect. Beginner hackers know how to bypass MAC filtering, but you could use it to stop less savvy neighbors if you want.

Firewalls:
If your team connects from home networks, the protection from the modem their Internet Service Provider gave them has limited security. Bear in mind that the ISP's primary goal is to eliminate compatibility issues with anything home users connect, so they avoid tight security controls that could upset a customer or cause more support calls. If possible, it is a great idea to

tell the firewall to block specific content. For example, you could tell it to block known malicious sites, sites known for phishing, and websites with content about drugs. You can block traffic from all countries except the ones you need. If you use cloud applications, you may be surprised which countries that software takes you to.

For a secure connection, your IT department might equip your remote employees with smaller SOHO firewalls for their homes that run behind the users' own firewalls. This can effectively isolate your users from the rest of their home network. If your employee must use a public network such as a coffee shop, your IT team can set up a hardware bridge to help protect their connection. Avoid the temptation to ask your IT team to examine and update consumer firewalls at users' homes, as that can be enormously time-consuming depending on how many users you have.

Passwords and Cloud Security:
It is essential that you implement two-step verification for all your users. In the most basic form, a person enters their username and password, and then their phone receives a text message with a code they enter to finish the login process. The idea is that even if a bad actor learns someone's username and password, they will not have access to the person's mobile phone. To save time and reduce frustration, some websites feature a checkbox to remember that device in the future.

It is essential that your user locks their phone and prevents an unauthorized coworker, family member, or any other person from gaining access to their phone. Use text messages if that is the only option, and know that, while difficult, attackers who know the password might gain access to the text message too. Other options for the second step include phone callbacks, physical USB hardware token keys, authentication apps on phones, and one-tap login solutions. Common choices include YubiKey, Authy, Duo, Google Authenticator, Microsoft Authenticator, and RSA SecurID.* There are many others.

Password managers are helpful; there are many pros and few cons. Ask your IT team their preference, and you may choose to allow your remote workers to use, or not use, password managers the way they do now.

Computer Security Updates and Firewall Patches:
One of the best ways to increase security is to stay current with the most recent security updates for computer operating systems and programs. Security patches for firewalls are often

overlooked with potentially devastating results. While at the office, your IT team can usually manage and deploy updates and patches. Your team might need extra tools to manage the updates on remote devices.

If your IT team won't have time to manage the remote equipment, it is common to configure remote computers and firewalls to automatically install critical security updates. A big pro is that you can be more secure from known security threats. One con is a slight chance that patches that install automatically might cause a user's device to malfunction. Security patches are so essential that you are probably better off applying them. Whether or not to apply updates automatically is a choice for executives to make depending on their risk appetite. Using golden images (see below) can reduce the potential negative impact of a misbehaved update.

Golden Image:
What if it is the middle of the night, or what if your IT team is unavailable, and the user's computer is malfunctioning? Ask your IT team to provide employees with an external USB hard drive containing a clean backup image of how their computer should be configured. If the worker’s computer malfunctions, show the users how they can reinstall the golden image the IT team created when the computer was new. When a user restores this "golden image," it is, from a software and operating system perspective, as if the user just received a brand-new computer. Beware that users must backup any local data files prior to restoring an image because the reset is so thorough that existing data will be removed. Another benefit is that if the user suspects there may be a virus on their computer, they can restore the golden image to reset the computer to a clean, fresh start.

Data File Backup to Local Removable Media:
Please do everything possible so that users do not need to store any local data on their computers. If they don't need to carry files to and from the office, and if they don't need data stored on their computer because it is on the network or in the cloud, that's the best scenario. But you may want them to be able to work from home even if their Internet connection fails, or there may be another reason you need them to have files stored locally on their computer. If that's the case, then the user should be able to back up their data files to local removable media. Examples include a USB memory stick or USB external hard drive. Your users need to save copies of their data files that are stored on their computer, if any, frequently. The duplicate copies of the files protect the user’s local data. If they need to apply a golden image, or if ransomware encrypts their local files, they need to have their important documents backed up.

It is essential that your IT team configure the backup drives so they are encrypted. It is too great a risk that one of the memory devices falls into the wrong hands and the data is compromised. Windows users can encrypt the devices with BitLocker. Note that if the user's home version of Windows isn't big enough to permit them to use BitLocker to encrypt their drives, IT can still encrypt the drives at work. Any version of Windows can access drives once they are encrypted with BitLocker. Mac users can use File Vault to encrypt an entire drive, but encrypting individual files is more secure on a Mac. There is another option for drive security that can be easier for your Windows and Mac users. Multiple vendors offer USB hard drives and memory sticks that have number keypads built into the device. Your users can literally type in a code to the device to lock and unlock the data.

Local Account is Standard User:

This is a crucial setting to stop hackers. Your IT team has hopefully had time to fix this setting on the company-issued computers. But if the user will use their home computer, someone needs to make this change on their personal device. Your IT team can fix this for them, making changes in the "control panel" under “users.” If you want to try this at home, the steps are: 1) Create a new user as a local account. Name it something like “Superhero.” 2) Change that user’s account type to be a local administrator. 3) Change your account type to standard. Now use your standard account from now on. Login to the account you always do. In case you have Mac users, the process is similar.

Reduce the Attack Surface:

Every program on a computer is a potential attack vector. The more programs you remove, the more secure a computer becomes. If the user is on their home computer, they probably have many non-essential programs. Attackers can exploit Flash and Java to execute malicious code, so it is best to remove both from all computers. Many people find that the websites that are essential work fine without Flash or Java. If they need Flash or Java again later, users can download fresh versions from https://get.adobe.com/flashplayer/ or java.com.

Computer Anti-Virus and Software Firewall Settings:

If your employees have company-issued devices, chances are that your IT team configures and maintains their anti-malware solution. If employees will use their home computers, they must be sure their anti-virus is working properly and is up-to-date.

It is essential that they configure the software firewall program component of their anti-virus product, or the software firewall built into their computer's operating system, to refuse all incoming connections. Some firewalls and Macs provide an option called “stealth mode.” When you activate this, you may get a scary warning that if you configure the computer to hide, it becomes difficult for outside parties to connect to the computer. Yes, that's the point! Block everyone. Nobody needs in except your IT professionals, and they already have a way in.

Physical Security:
If an attacker gains physical access to a user's laptop, computer, phone, tablet, or other devices, compromising the security is magnitudes easier. Calculate the impact if a user’s device is compromised, allowing attackers access into your network. The repercussions to your organization might be devastating. If necessary, provide your users with pick-proof locks for their doors. You can ask them to take photos of their home locks to send to you, and you might want to send a member of your facilities team, or a specialist, to examine their home's security.

Sometimes companies issue outside security cameras and inexpensive alarm systems to their employees. While those sound like a good idea, they primarily detect, not prevent, break-ins. Deterrents are certainly good, including alarm stickers on doors and windows. But remember to implement preventative controls including high-quality deadbolt locks, reinforced door jambs, and sliding door security bars. Exterior motion-sensing flood lights can be very effective too. Having tight security can even enhance your employees' and their family's personal safety. Giving them added peace-of-mind during this crisis is helpful.

UPS Battery Backup:
If the coronavirus response becomes very serious, it is possible users might experience loss of power. If there is a loss, hopefully it will be short. Consider providing battery backup devices to users with desktop computers, printers, and home modems. If the user has a charged laptop and a charged battery-powered hotspot, and no printer, the battery backup is often unnecessary.

Special Security Training about Coronavirus:
Warn your workers that there will be an increase in spam and phishing as bad actors prey on their worries of the virus. They must be vigilant to spam and fake news. Recent hacks provided attackers with detailed information about families and histories, so that phishing can be more convincing than ever. Manually visiting, rather than clicking links to, ready.gov and CDC.gov contain information about how to prepare and find status updates.

Test Remote Access:
All of your users need to engage in a “pretend it is real” run through. Once they are configured, they need to test performing all of their job functions working from home to be sure everything performs as expected. Solve problems that come up. If one user has an issue, take preemptive action to be sure it doesn't happen with the others. This is too important to not test out ahead of time. Your workers may wake up one morning and find out they have to stay at home that day. Every night they need to take what they'll need to work from home just in case. If they are able to come to work the next day, they'll need to haul all that stuff back and forth. Minimize as much as possible what they'll need to take.

Additionally, give your employees guidelines on what to do if they lose connectivity to the office, and what to do if they feel like their remote computer might be under attack. Consider that, if your IT team is busy tackling bigger challenges, they may not be available to help that user right then.

Show Extra Gratitude to IT:
Finally, throw a big party for your IT team that made all of this happen. Chances are they've invested more energy and patience than you know because they make it look so easy. Tell them that you recognize the amount of expertise they needed to get you to the point of accomplishing this list. A little gratitude goes a long way.

All your preparations are worth it. The World Health Organization is already saying there will be more viruses in Earth's future. You are preparing for the future too. Good job implementing these recommendations now. The increase in the number of people who must work from home because of coronavirus could accelerate quickly at any time.

If you have any questions, please email mike@fosterinstitute.com

Please forward this to your friends so they can prepare their organizations too.

*The Foster Institute, Inc. does not receive any compensation from, nor does it endorse, any products or companies mentioned in this article.