Protecting Yourself from Cyber Threats in a Telecommuting World

The Novel Coronavirus has altered much of how we go about our work and daily lives. One of the most notable changes in the workplace has been the widespread surge in telecommuting as many employers have encouraged or required their staff to stay home in order to practice social distancing. While this sudden shift has presented a wide array of challenges, the issue of cyber crime has emerged as one of the most immediate and daunting threats facing the average remote worker.

The unfortunate reality is that cyber crime is on the rise as a result of the current pandemic. The World Health Organization (WHO) has already reported a fivefold increase in attacks targeting its employees since the beginning of the COVID-19 outbreak. Cyber criminals have always been ruthless and opportunistic in their attacking of vulnerable entities, so it is no surprise to see an increase in this activity as we all attempt to operate in this uncharted territory. Individuals and organizations alike are scrambling to adapt to the new “normal,” and cyber criminals have been quick to exploit the situation.

This has been clearly displayed in the significant uptick of phishing emails in circulation. You have probably noticed a constant stream of notifications from your banks, dentists, retailers, etc. alerting you as to how they plan to operate during the pandemic. Cyber criminals have seized on this moment, impersonating trusted sources as they slip into the ranks with their own COVID related emails. Most phishing scams attempt to entice victims to surrender personal information or download malicious software by creating a sense of urgency or fear in the victim, so the current uncertain times have proven to be fertile ground for such attacks. It is now more important than ever to be vigilant in protecting your computing systems – particularly with the added exposure that telecommuting can bring.

The same basic cyber security principles apply both to employees working in the office as well as to those working from home. What typically makes securing remote workers more challenging is simply the fact that the organization has less control over the remote environment and the volume of work taking place online tends to increase substantially when workers are telecommuting. This makes it imperative that telecommuting organizations have a robust cyber security program in place and remote workers are well trained on organizational policy. However, the unexpected nature of the Coronavirus pandemic has forced many employers to quickly accommodate a makeshift system of remote work and has relegated the idea of employee training to the bottom of the priority list. Unfortunately, cyber criminals are not sympathetic toward entities struggling under the strain of these unprecedented times, so it is up to you to protect yourself and your employees from a cyber attack. Here are some key items to consider when establishing cyber policies and training for your telecommuting employees:
IT Support

As more of your staff begins to work remotely for the first time, you can expect an increase in employees needing technical assistance. Ensure that you have adequate support from internal staff or from an outside IT vendor.

Separate Personal and Work Devices

Ideally, employees should use different devices for work and personal purposes. This helps prevent the risk of a cyber infection caused by personal activity from spreading to work applications by separating personal and work use to their respective personal and work devices. Supplying employees with specifically designated work devices also gives employers a greater extent of control over the devices and allows them to ensure they meet minimum security requirements.

Secure Networks

Remote employees must be restricted to only using secure networks. One of the most often touted perks of telecommuting is the ability to work from almost anywhere, but employees should never be allowed to connect to public WiFi provided at many cafes, libraries, or other public areas for work purposes. WiFi networks that require a password indicate that they are encrypted which helps keep the information safe that is transmitted over the network. Still, even some encrypted WiFi installations are outdated and potentially dangerous. Currently the safest encryption type is WPA2 which can be selected in the router settings. Employers should verify that their remote workers have access to a secure network or provide a HotSpot in the event that secure WiFi is not available.

Least Privilege

The principle of least privilege is the practice of limiting the access rights of users to only the computing systems and resources that are absolutely necessary for the work that they perform. Employees should be given the minimal level of user rights or lowest level of clearance that is needed for their respective roles. The concept is simple – if you reduce the number of people who can access a particular system, you also reduce the likelihood that the system and corresponding data are compromised by a security breach. Your most sensitive data should not be accessible remotely, but if it is not possible to restrict it completely, access should certainly be limited to the greatest extent possible.
Physical Access

While it may feel like cyber crime is constrained to the virtual realm, all cyber attacks originate in the physical world. That is why it is important to pay attention to the physical access of computing systems. It is likely that your servers are kept behind locked doors where only your IT staff can access them. Your employees may be diligent in logging out of office devices when not in use or shutting down office computers at the end of the day, but what about when they are working remotely? It can be easy to relax security measures in the privacy of one’s own home; however, employees should be reminded that the same security standards apply in a remote workspace. Devices should always be locked when not in use as a protective measure against tampering in the event that the device is lost or stolen. Preferably, they should be set to lock automatically after just a few minutes of inactivity. Even a child or roommate can inadvertently introduce a virus to an unlocked work computer while attempting to surf the net or install a game.

Updated Systems

The cyber landscape is always evolving. Cyber attacks have become more sophisticated over time, but security features have advanced as well. System updates often contain critical security patches meant to shield us from the latest attack, but they will not do any good if they have not been installed. Many programs run automatic updates without needing input from the user. For example, the popular browser Google Chrome downloads updates automatically; however, those updates will not take effect until the program is restarted. Employees should periodically close applications and restart their devices in order to allow proper installation of system updates.

Data Backups

Backing up your data is a critically important piece of any cyber security program. If you experience a cyber breach, your only course of action may be to wipe your entire system and bring back your most recent backup. Ensure that your backup strategy includes and is clearly communicated to your telecommuters. Remote work can often be more cumbersome than traditional office work due to the added necessary security features such as limited system access or the use of a VPN. A common tactic employees use to bypass these features that they deem inconvenient is to simply download the documents they need and work on them locally. Employees must understand that any work done locally will not automatically be included in a system backup.
Video Conferencing

During this time of distancing from coworkers, friends, and loved-ones, video conferencing platforms have exploded in popularity as a way to stay in touch. Unfortunately, they have also attracted their fair share of bad actors. Many reports are emerging of a new phenomenon known as “Zoom-bombing” (a term coined from the widely popular Zoom video conferencing app) where attackers hijack a conference call and are able to listen in on a call, heckle attendees, or display derogatory or pornographic images on shared screens. Employers should take precautions to ensure that they are protecting themselves and their employees when using video conferencing services.

- Only use credible, encrypted video conferencing apps.
- Do not cut corners on security. While many video conferencing apps offer free versions or trials, most offer paid alternatives with business-grade software that typically provide more security features.
- Password protect your meetings if possible.
- Do not share teleconference links via social media post. This may feel like the quickest and easiest way to reach a large number of your target audience, but links shared publically can easily be exploited.
- Ensure you are using the latest software version. Software updates are important for your security as noted in the “updated systems” section. Due to the ongoing appeal of video conferencing for both legitimate and malicious purposes, much focus has been put on updating this software in order to close security loopholes.
- Do not allow attendees to join a call before the host. Most conferencing software has a waiting room feature for this purpose.
- Lock a meeting when all attendees have joined. This prevents unwanted eavesdroppers to join; although, you will have to unlock the meeting for a valid participant who has dropped out of the call to rejoin.
- Pay attention to recording and other settings, and only record a meeting if you need to. Thousands of recorded Zoom meetings recently surfaced on the internet. However, Zoom's servers had not been breached. The issue occurred because the videos were being saved to users’ cloud storage services, and the recordings were saved using the default naming settings making them easy for cyber criminals to find.

Phishing Emails

Phishing is a cyber scheme in which the attacker sends a fraudulent email that appears to come from a credible sender to a victim in hopes of introducing malware to the victim’s system or enticing the victim to reveal personal information. The vast majority of cyber breaches begin with a phishing attack, and while phishing can occur in various forms including texts and phone calls, phishing emails have long been the most common approach. As previously noted, there has been a significant increase in opportunistic
Phishing attacks since the pandemic began. It can be tempting to mix work and personal email accounts when working from home, but telecommuters should never use a work account for personal emails or vice versa. In addition, all employees should be trained to spot and avoid suspicious emails, and they should be given an IT contact with which to share those messages for evaluation purposes.

Phishing emails are intended to appear as though they have come from a trusted source. As many as 20,000 college students experienced a recent phishing attack in which they received emails seemingly from university leadership requesting that they click on a provided link to review COVID-19 related information. After following the link, they were asked to provide their usernames and passwords to access the content, but this was just a scam to steal account information. In these unprecedented times where pandemic related information is constantly being shared and leadership is finding it necessary to communicate more often with more staff members, it is more important than ever for employees to follow these defensive tactics in order to avoid phishing attacks:

- Examine the email closely. Look at the actual email address, and not just the name of the sender. Inspect all links. Fake addresses are often only off by one or two letters.
- Phishing emails can also come from legitimate accounts that have been compromised. If you recognize the sender, but are suspicious of the message content, pick up the phone and call the sender to verify that the email is credible. If you receive an unexpected mass email from leadership similar to the university example above, ask your immediate supervisor to confirm the validity.
- Be especially cautious when emails ask you to take actions such as opening attachments, downloading programs, following links, or inputting login credentials.
- Exchange personal information over the phone rather than by email. If you receive an email from a doctor’s office or credit card company seeking personal information, respond by calling rather than replying by email to the institution.
- Put yourself in the driver’s seat online. The internet can be a dangerous place. You want to be in control of your actions online rather than responding to items put in front of you. Even if you receive an email that appears to be credible from a source that you know, such as a notification from your bank asking you to verify account information, get in the habit of closing the email and going to your bank in the search bar rather than by following any included links. If the email was legitimate, you will still be able to update your account accordingly by visiting the website yourself without following the link included.
Passwords

Guessing or hacking passwords is a common way that cyber criminals gain access to a computing system, making it crucial that password requirements are clearly outlined in organizational policy. Consider the following best practices for creating secure passwords:

• Password should be long – It is recommended that passwords be at least 10 characters in length. The longer the password, the more unlikely it is to be guessed or cracked in a brute force attack.

• Password should be complex – Passwords should also contain a variety of characters (capital and lowercase letters, numbers, and symbols) in order to decrease the likelihood that a password is cracked.

• Password should be unique – Do not use the same password across multiple accounts. If your login credentials are exposed during a cyber breach of a particular website or program, but you are using the same username and password for multiple accounts, the cyber criminal will now have access to any other account that you have registered for using the same credentials.

• Password should be changed regularly – There is a large market for stolen personal information. If an organization where you have an online account experiences a cyber breach, your login credentials could be exposed, but they may not end up in the hands of the end user for several weeks or months. If you have changed your password in the meantime, you have rendered your old credentials worthless to the thief. Changing a password also prevents prolonged access as a hacker may attempt to access an account more than once over a period of time.

Cyber Incident

It is crucial to respond quickly to any cyber security incident. Many times a minor incident can increase dramatically in cost and complexity simply because it has been allowed to languish. It is possible to limit the damages and isolate the infection by acting fast, but often employees have not been trained on what to do. Employees may choose to ignore the issue fearing discipline and hoping that it resolves itself while no one notices. In some cases they may even exacerbate the situation by trying to find their own solution online such as downloading free PC Cleaning software. Ensure that employees have been trained to report suspected cyber incidents to a designated contact. Also, be sure to contact VACORP as soon as possible with any potential claim.
Additional Support

VACORP’s Cyber Security webinar is available for training purposes at our website, VACORP.org. This provides information applicable both at home and at work. In addition, members who purchase increased Cyber Risk limits have access to our cyber security portal, eRisk Hub. To access this portal, simply log into your account at VACORP.org and select “eRisk Hub” from the dropdown list under the “Resources” tab. This will open a new tab in which you will have access to a wealth of resources including interactive tools, training videos and simulations, policy templates, self-assessment, and much more.

Please contact your VACORP Risk Control Consultant or Member Services Specialist for more cyber security risk management tips or information regarding your Cyber Risk coverage.