COVID-19, Work From Home, & I.T. Security

With remote work strategies increasing and introducing completely new workflows into our daily habits, this brings new vulnerabilities for attackers to exploit. We must continue to remain vigilant.

To that end, please keep the following guidelines in mind and share them with your teams:

**Remote Access Safety**

**Remote VPN Access**

With the Coronavirus forcing many businesses to work remotely, the utilization of VPN circuits to connect users to corporate networks is necessary. Here are best practices for remote VPN access:

* Systems utilized for remote access need to be provided by the business. Do not allow personal computers (not provided by the company) to connect to the corporate network.
* Make sure that systems that are allowed to connect remotely are patched up-to-date.
* Make sure that network devices providing VPN remote access are also patched.
* If using a VPN, you should also utilize multi-factor authentication or two-factor authentication to protect the connection.
* Be cautious of home networks, other systems on the network, and wireless access when using a VPN channel from home. Maliciousness can spread from a home network to the corporate network via the VPN channel.

**Avoid Public Wi-Fi**

With the current situation, not many public areas are even available. But there are some. Be extremely cautious when accessing your corporate network through these types of connections. Your home Wi-Fi can be considered public if not properly secured. So always use the company-recommended methods of secure connectivity (VPN, VDI, etc.).

**Encrypt Sensitive Data in Email**

Email sent from one company member to another is always safe (its automatically encrypted). When an email is sent outside of your company (not encrypted) that email is called “Open Text”. Anyone that can capture it can read it. Always send important “Sensitive” emails in an encrypted format. If you don’t know how, reach out to your company’s I.T. team or help desk for instructions.

**Surfing Warning: Sharks in the Water**

Be extra cautious when surfing the internet remotely. You may not be under the protection of your company’s web filter and could put your system at risk. Only visit sites you know and trust.

**Outside Threats**

Criminals will continue to attempt to spam, phish, and social attack you and/or your computer. Maybe even more so when working remotely. Attackers are hoping you’re not as diligent when at home. Always keep your guard up and be aware. If you identify some level of attack, contact your I.T. team or help desk immediately.

**Email Threats**

**Confirm Senders**

Email phishing scams often include showing a colleague’s name in the “To” field; however, when you look more closely it is from a different email address. Be sure that the sender is the correct email address. Don’t just rely on the name that is displayed.

**Beware of Urgent Calls to Action**

If an email is asking for you to take quick action, BEWARE! Best practice is to contact the sender in another form and confirm that they sent you the email. An urgent call to action is one of the most common means of preying on colleagues who only want to be helpful.

**Texting and Phone Calls are Fair Game**

Texting and phone calls are not off limits when it comes to an attack. If confidential or other sensitive information is requested from you over the phone, tell the caller you will call them back before giving them that information (or follow your company policy in handling that information). Never give information to someone who can’t be called back on a known number. This holds true even if you recognize their voice. Verify, verify, verify.

**Don’t Click on Unexpected Links or Attachments**

Attachments or links is how your computer gets compromised. If you’re sent a link or attachment, contact the sender and verify that they sent you the link. However, do not use the contact information in the email to verify (it could be fake). Look the contact information up elsewhere and contact that sender.

**Verify Website Addresses**

In a rush, we all can make the mistake of leaving out the “m” in a “.com” website. Be aware that “.co” is real. Your favorite sites could easily have been copied by an attacker who is trying to steal your login information on the “.co” website they control.

**Some Physical Security**

**Lock Your Home**

This is Security 101: if you bring your work computer home or tend to work remotely, confidential corporate information could be at risk. When you get in the habit of always locking your doors, you have taken a key step toward improving your home office security.

**Never Leave Your Devices or Laptop in the Car**

We advise our clients and employees to never leave their work computers or devices in a vehicle. It’s best practice to keep work laptops and devices on your person at all times when working remote.

**Don’t Use USB “Thumb Drives” That You Don’t Know Anything About**

Never use a thumb drive if you don’t know where it came from. Borrowing a USB drive from a family member or a friend may introduce malicious actions on your company provided, remote computer. If you are not familiar with the device, then avoid it.

**Company Computers Should Only be Utilized by Company Personnel**

Don’t let family or friends use your company provided computer. What is accessed by that computer system while in your care is your responsibility. Keep your company systems close to the chest. It is for your access only.

We must remain diligent in this unprecedented time to ensure the continuity of our businesses. If you feel that a request or email is unusual in any way, please verify that information before you proceed. You are not wasting anyone’s time. You are protecting yourself, your colleagues, and your company.

Original Source: ABA endorsed partner Netgain