Best Practices for Securing Your Home Office

CMIT Solutions®
Your Technology Team
Cleveland East & Southwest

General Tips

- Use a power strip rather than plugging computer cord into wall.
- Ensure you are connecting to your private Wi-Fi which should be password protected.
- If you have not changed your Wi-Fi password recently, it would be a good idea to do that.
  - Recommended never to connect to a network unless it is password protected (ex: public Wi-Fi at Starbucks). Use your Personal Hotspot on your cellphone rather than public Wi-Fi.
- If you're working from home and have the ability to set up two networks on your router, it is recommended to configure one network for the computer you use for work and the other network for all other devices.
  - Use different names – unrelated to you or your business … like WR32B for your work computer and WR32B-XYZ for all other devices.

CMIT Solutions® Your Technology Team

Cleveland East & Southwest

General Tips

- Check with your company's IT department about their policy regarding using a "work computer" vs "personal computer you are using for work purposes".
- If you are using a personal computer for work, ensure you are keeping up to date with security and operational updates from third party vendors such as Microsoft and Adobe.
- Ensure the personal computer has anti-virus protection and all updates are current.
- If you are sharing a personal computer with family members, it is recommended to set up separate User Profiles.
- If you have a smart speaker like Amazon Alexa, Echo, or Google Home, it is recommended to unplug those devices when you are having business conversations.

Passwords

- Make strong passwords that don't include personally identifiable information (i.e. kid's names, birthdates, etc.).

- In 2018, the US Department of Commerce's National Institute of Standards and Technology (NIST) released new guidelines recommending a shift away from password complexity and toward user friendliness. The NIST guidelines now call passwords "Memorized Secrets" and recommend that users create long passphrases that are easy for them to remember instead of convoluted strings of nonsensical numbers and letters. The use of special characters—!, @, #, $, %, and the like—is still recommended by the guidelines, and they encourage online platforms and accounts to allow log-in credentials to stretch up to 64 characters to support the use of such long passphrases.

- Best practice: Don't allow your browser to save passwords or to auto-login.

Passwords and Multi-Factor Authentication

- Best practice – Do not save your passwords in a Word or Excel document on your computer. If you MUST do so, do not name it "Passwords". Name it something like "Mom's Soup Recipe" and do not use the word "password" anywhere in the document itself (it will show up in a search). Password-protect that document, so if someone else tries to open it, they can't do so without the password.

- An option is the use of a password manager which is essentially an encrypted digital vault that stores the login information you use to access apps on mobile devices, websites and other services. Some examples: LastPass, 1Password, etc.

- Use Multi-Factor Authentication whenever possible as an extra layer of protection beyond just the use of a password. MFA requires something you know (your password) with something you have (a unique code delivered via text message or email). You can also set up an authenticator app, such as Authy or Google Authenticator.

Video Conferencing

Video Conferencing services such as Zoom, GoToMeeting, and Webex have become very popular with so many people working from home.

- It is being reported that there are threat actors sabotaging this new way of conducting business by using public links to hop on meetings to shock, taunt or scare users. Here are a few tips to avoid that:
  - Avoid sharing meeting links publicly on social media
  - Avoid using a Personal Meeting ID to host events
  - Hosts can generate a random Meeting ID and require a password to join
  - Use the Waiting Room feature which allows the host to approve participants
  - Allow participants only to join using the email through which they were invited
  - Lock the meeting once all invited participants have joined
  - Check the microphone and video settings as soon as you log in to ensure they are set to how you prefer for that meeting

Detecting Phishing

- Don’t trust the display name of who the email is from … Hover over parts of the email.
- Check for misspelling, bad grammar or unusual phrasings.
- Consider the salutation – is it general or vague?
- Is the email asking for personal information? Is there a sense of urgency in the email?
- Check the email signature – most legit emails have a full signature block at the bottom.
- Do not click on links or attachments from unknown senders (beware that some emails appear to come from known senders, so be vigilant with these tips mentioned).
- When in doubt, call the person first and ask them if they sent the email.
- Be aware of “text phishing” and also “voice phishing” where hackers mimic the voice of people you know in hopes you will reveal confidential information.

Backup is Critical

- No matter where you are conducting business, it is critical to have regular, remote, redundant, monitored and **secured** data backups.

- If you are backing up work-related data, keep in mind that files you copy to your "personal computer" may represent a breach in confidentiality or compliance.

- Understand how to access and save data correctly to avoid any potential problems down the road. Check with your IT Provider to see if data you create or modify is being backed up and managed correctly.

- Ransomware is when hackers take your data hostage until you pay a ransom to get access to your data back. Having a proper back-up solution is critical for many reasons especially if your business is a victim of a cyber attack.

If you're interested in seeing how ransomware can happen, check out this video "Ransomware – Anatomy of an Attack" … https://www.youtube.com/watch?v=4gR562GW7TI&t=108s

Additional Ways to Stay Secure

- Lock your computer when walking away.
- Use a camera cover at all times (except on video conference).
- Never send confidential information via email or text. It is recommended to log on to a secure portal or use encrypted communication tools.
- Be careful about the information you share on social media as hackers use that information for passwords, text, voice and email phishing scams, ransomware, etc.
- It is recommended that you do not check the box to save your credit card information for future purchases.
- Make sure you are using secure websites – it should have http**s** (unsecure websites don't have the "s" after http) or there may be a lock symbol showing it is secure.
- If you suspect you may be getting hacked (maybe you clicked on something accidentally), immediately disconnect from Wi-Fi and/or unplug your ethernet cord that is hardwired to your internet.

Why It Is Important for Businesses To Stay Secure

- It is predicted that by 2021, cyber crime will cost the world $6 trillion annually.
- On average, there is a hacker attack every 39 seconds.
- 1 in 323 emails sent to small businesses are malicious.
- Over 80% of cybersecurity breaches can be traced back to human error.
  - Increased investment in employee training can significantly reduce the risk of a successful cyber attack.
- 60% of small businesses go out of business within 6 months of a cyber attack.
- Cyber attacks are on the rise during COVID-19 crisis.

CMIT Solutions®
Your Technology Team
Cleveland East & Southwest

We hope you and your family remain safe and healthy.

If we can be a resource for your business, please contact us.

440-462-7500

https://cmitsolutions.com/cleveland-east-southwest/

Ed Cordiano
ecordiano@cmitsolutions.com

Mary Ann Cordiano
mcordiano@cmitsolutions.com

Let us know if you would like to receive our Weekly Quick Tips.