Seal Cyber Tech, LLC
https://sealcybertech.com
(904) 834-1246
1646 Rogero Rd
Jacksonville, FL 32211

Cybersecurity Tips to Working Remotely from Home

1. Update your Operating System and Applications. If you are working from a personal computer, and IT personnel do not maintain your computer, it is best to take it upon yourself to keep all your software updated. This will help patch up known security vulnerabilities. This can be setup to happen automatically.

2. Go online through secure networks. It's tempting to use free Wi-fi access to access the internet, but insecure connections can transmit your information in plain text. If you must use a freely available Wi-fi connection, try to always use a VPN to encrypt your activity. Your company may provide a list of approved VPNs to use. Particularly if you access company resources through the internet, you should use a VPN to avoid eavesdroppers.

3. Use strong and different passwords for accounts. It is very common to use the same password over and over again on many accounts. The problem with this practice is that if one account gets compromised, then potentially all your accounts are compromised. You should also frequently change your passwords. To help with the problems of memorizing many different passwords, you can use a password management application.

4. Use multi-factor authentication to login to accounts. Yes, it is an extra step, but it also protects your account from unauthorized access. All the big companies have it. A common tool today to use as an additional verification to login to an account is your smartphone. The system can send you a pin via text message or better yet, a pin through an authenticator app.

5. Try not to open links from emails unless they are from a trusted source. Have you ever received a phishing email that looks just like one that you received from a bank? Many times, if you try to mouse over the link, you will see that it will take you to an address that does not belong to the bank. You can also check the source email. If it doesn't look right, avoid clicking on the link. So in essence, verify emails and links before sharing confidential information. Be vigilant and if necessary, paranoid. It's better to make a quick call to confirm, rather than lament.

- IT will never ask you for your password
- IRS will never call you (they usually send mail)
- No Nigerian Prince will want to give you $500,000 for assisting in a transfer

6. If you use a home router, it is important to secure it. First make sure the default password is changed and safely stored. Second make sure you are using WP2-PSK (AES) or higher is possible. Also, it is important that you turn off file sharing on your personal computer when used for work. This will avoid shared folders through your home network.

7. Make sure your hard drive is fully encrypted. Particularly if you use a laptop. In Windows, it is common to use Bitlocker, in Mac OS it is common to use Filevault.

8. It is not recommended that other people use the same computer or network. If several people use the same computer, make sure that each have their own account and that they don't have administrative access to go through your files. It is recommended that you have the proper ACL controls to limit other users from accessing your files. VLANs can be used to separate networks. You can create one VLAN for your kids to browse the internet and another for your work.

9. Make sure your screen auto-locks after a short period of time. If you leave your desk temporarily, you don't want just anyone to see what you were working on or actually use your computer. If you know you will take a lunch break, just logout.

10. Backing up important files is a great practice, but if you backup to the cloud, make sure to encrypt the files or at least password protect them. For example, if you use Google Drive to save documents, you can use Bcrypt to encrypt your files and avoid others from potentially looking at private company documents.

11. Remember to use and update your antivirus software. Let it run daily or at least weekly scans during the night, so it doesn't affect your work.

12. If you are connecting to a computer in your corporate office, you may be using a VDI (Virtual Desktop Interface). It's basically a virtual computer running on a server controlled by your company. This is a really great option, as the IT Team will make sure it is secure and will most likely provide you with a VPN to connect to this Virtual Machine.
13. Always remember that while you are connected to your office, you are potentially being monitored.

14. Practice wiping empty space on your hard drive. Information you delete from the trash can still be recovered.

15. Always report any suspicious activity that happens while using your computer to the IT Staff.

16. Turn off or remove smart speakers (ie Amazon Alexa, Apple Homepod, and Google Home) from places you have private meetings. These devices are meant to record you.

17. For online video conference calls, make sure your microphone and camera always default to off. Turn them on when needed. Also remember to put passwords on all conference calls.

If you need assistance with any of these items, contact us at sealcybertech.com.