XANTRION

10 Tips to Work from Home - **SECURELY**

1

Phishing scams are rife.

Be aware of phishing scams targeting remote workers with sensational or emotional messages. Without your colleagues around, you need to be extra vigilant of both email and phone scams. Never click on an attachment you weren't expecting.

2

Be extra careful of fake news and malicious websites.

Now more than ever "click bait" content is running rampant taking advantage of newsworthy events, such as the COVID-19 pandemic.

3

Your passwords are the key to the kingdom.

Without the company network to protect you, the power of protection lies squarely in your hands and depends on the passwords you choose. Make sure your passwords are unique and strong. You might even consider using pass phrases. Check your policy on password managers and use one if allowed.

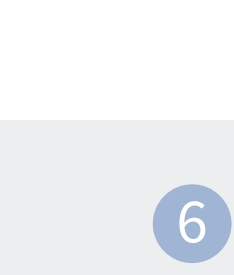
4

Use Multi-Factor Authentication wherever possible.

MFA combines your username and password with something you own, such as a One Time Password app on your phone. MFA reduces funds transfer fraud, blackmail and identity theft by a factor of 1,000.

5

Don't fall for "credential phishing" attacks,



where scammers trick you into handing over your usernames and passwords. It's best not to click on links asking you to update details. Instead, bookmark the sites you frequently visit.

6

Implement basic security measures.

Use the latest software. Keep your operating system, plug-ins and antimalware up to date. Turn on automatic updates if you can.

7

Secure your home WiFi Network.

There are 2 basic must-dos to set this up securely. Change your default router password if you are still using "admin/admin", "admin/password" or something similar when you log into your router.

Next, when setting up a password for your WIFI network, make sure you choose WPA2. And whatever you do, don't run a wifi network without a password.

8

Keep your work environment private.

Ensure nobody is allowed to access your work computer, including your kids. Others could unintentionally download malicious software or see documents they shouldn't see. Ensure your work conversations remain private and turn off smart devices like Alexa. If you walk away from your device, lock it.

9

Store files in a secure cloud location

rather than on a local drive or removable media. Secure storage, such as SharePoint Online or OneDrive for Business, ensures even if your physical device is lost or stolen, your data is available to you and your company.

10

Follow your policies.

Resist the temptation to use unapproved software or store data outside company resources. Now is the perfect time to let IT know if you need something you don't have. Shred work documents.

Xantrion | 651 20th Street | Oakland, CA 94612 | 510.272.4701