A Guide to Securely Working from Home

Unfortunately, during times of crisis hackers try to exploit organization's weaknesses and aggressively target employees who are often the weakest link in the security defenses. The current coronavirus crisis has forced organizations to provide remote access to their employees so that they can continue to partially operate while also complying with the social isolation and social distancing mandates. Every employee needs to be vigilant and know that they play a critical role in ensuring that their organization does not fall victim to a data breach during these extremely challenging times. Below are some tips to assist you in keeping yourself safe and secure.

- Be extremely vigilant for phishing emails, suspicious phone calls and malicious sites.
- Lock your computer whenever it is left unattended.
- Be conscious of who is able to see your computer screen(s) when viewing sensitive information and of who may overhear sensitive phone conversations.
- Avoid using personal devices, such as tablets or laptops, for business purposes, unless specifically authorized to do so by IT.
- Limit use of company-issued devices for personal activities.
- Never use your personal email, cloud storage, such as Google Drive, Dropbox or iCloud or social media accounts to access or share information.
- Do not use communication or chat platforms that are not authorized by the company to discuss business topics.
- Do not download software onto any devices used for business purposes unless specifically authorized to do so by IT.
- Use company provided cloud storage to minimize the need to store data locally on your computer or on any removable storage devices.
- When you are participating in a videoconference please be cognizant of any sensitive information that could be inadvertently viewed by the other participants.
- Use an additional verification step such as a phone call to confirm any requests for access to sensitive information, financial transactions, account credentials.
- Use multi-factor authentication (MFA) to access all company resources as directed by IT.
- Use a virtual private network (VPN) to access all company resources as directed by IT.
- Make sure that your home network is secure and that your wireless router has up to date software and is not using the default admin password.
- Do not allow family members the use of your company provided computer and devices.
- Avoid printing sensitive documents for use at home. If you must print a document, ensure it is stored securely and destroyed (shredded) after use.

Additional information on securing your home network can be found at https://www.sans.org/security-resources/posters/creating-cyber-secure-home/80/download