TAKING SECURITY HOME

Working Remotely & Securing Your Home Office

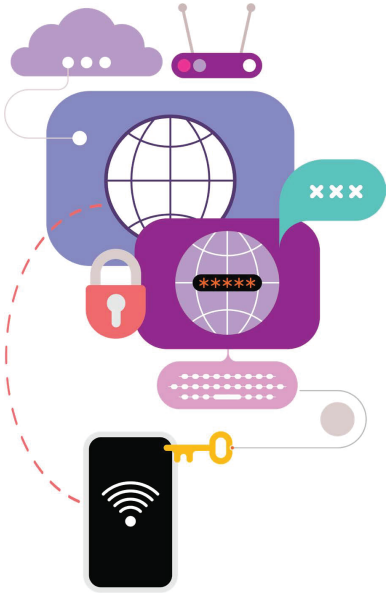
Make security a priority with the following guidelines -

Stay Committed to General Security - Organizational Policies Still Apply

Working away from the office does not exempt anyone from following policies, which were designed to prevent data breaches and to maintain the privacy of our employees, customers, clients, and business associates. Circumventing policy in any way undermines those efforts.

Separate Work and Personal Data

Use organization-issued computers and mobile devices for work purposes only. If you don't have an organization-issued device, be sure to check our policies about using personal devices to access our organization's data or networks, and consider creating separate user accounts, which will allow you to isolate work accounts from personal accounts by setting up specific logins for each.



Secure Your Home Network Awareness

If you haven't already, update the username and password of your router immediately. Most routers ship with default login credentials that are public knowledge, which means anyone within range could log in and change settings. Protect your network with a strong, unique password. Obviously, never use the same password for your network and your router. If you need help with general router maintenance or advanced network security options, there are plenty of "how-to" guides on the web that offer great advice in easy-to-understand language...**or contact us with any questions.**

Helpful Tips

- Update software, and enable automatic updates where available
- Think before you click!
- Remain skeptical of all requests for sensitive information
- Shred or destroy sensitive documents before discarding or keep secured until coming back into the bank to shred (Clean Desk Policy)

VPN

Use a virtual private network (VPN). A VPN is software that encrypts your internet connection and prevents others from viewing your internet traffic. SSE requires all employees to use our VPN to access the SSE Network.

Lock your workstation. When not in use, always lock your workstation and ensure no one else in your household can access work-related information or accounts.

Beware of smart devices. Ensure voice-controlled smart devices can't listen in on any discussions that involve confidential information. Ideally, remove smart devices from your workspace.

Watch out for phishing scams. Cybersecurity experts warn about phishing scams tied to the pandemic. These emails are designed to take advantage of people's curiosity.

Working from home will continue to grow in popularity as more and more organizations embrace remote culture. So, we also need to embrace remote security to maintain the privacy of our employees, customers, clients, and business partners.

If you have any questions, please ask!
(314) 439-4747

SSE