Click Thinking Spotlight

Working at home

If you work from home, there are things to keep in mind that will protect you and your company from data loss and cyberthreats. The following tips will help you steer clear of them.

- Designating a place for work devices and things like usb drives with company data lessens the chance they'll be lost or stolen.
- Never leave written passwords out where they can be seen. In fact, if you can, commit them to memory so they can't be compromised.
- If you must write them down, insert random characters only you know to avoid. This will prevent unauthorized users from logging onto your network.
- If your company uses security tokens, keep them with you at all times or store them out of site when not in use.
- When you step away from your device, remember to lock your screen so no one can use it. Setting the auto lock feature can protect you if you forget.
- For longer periods of inactivity, secure your device away from the eyes of tempted children or visitors.
- If you work on a family computer, log out of all work-related networks and applications when finished to prevent unauthorized or accidental access.
- Never share your network or piggyback on a neighbor's wifi as cybercriminals may use the connection to gain access.
- Use a Virtual Private Network, or VPN, to send and receive work emails if your company doesn't already use one.
- Most companies have strict policies to ensure security for those who work from home. Be sure to obey these policies or consult with your manager or human resources if you have questions.

Working From Home

For the animated training module on this topic, see your manager or information security contact.