Keep Work Separate Designating a place for work devices and usb drives with company data lessens the chance they'll be lost or stolen. A designated space also says 'stay away,' reducing the likelihood that someone might mistakenly take or access your devices. **Guard Your Passwords** Never leave written passwords out where they can be seen. If you must write them down, insert random characters only you know to avoid. Never share your passwords with family members, and change them periodically if your workplace doesn't prompt you. Keep security tokens out of reach. **Lock Up And Log Out** If you work on a family computer, log out of all work-related networks and applications when finished to prevent unauthorized or accidental access. For longer periods of inactivity, secure your device away from the eyes of tempted children or visitors. **Safeguard Your Home Network** Be sure your home's internet is dedicated and secure. Never share your network or piggyback on a neighbor's wifi. Use a Virtual Private Network, or VPN, to send and receive work emails if your company doesn't already use one. Doing so will encrypt your communications so no one else can read them. **Practice Policy** Most companies have strict policies to ensure security for those who work from home. Be sure to abide by them.

WORKING FROM HOME • CYBERSECURITY FROM A DIFFERENT PERSPECTIVE