On the Job *but* Out of Office

Working remotely has opened new ways for cybercriminals to steal information off laptops, smartphones, and tablets. The result is increased cases of identity theft, stolen documents, and substantial financial losses for employees and employers. Let's fix that!

Slow down.
A study by the University of Central Florida says that when we bypass our employers' security policies — often because we're trying to get work done faster — we are far more apt to suffer a cyber breach.

Use work devices for work. Use personal devices for personal stuff.
That minimizes the amount of information an attacker can access and prevents family members from accidentally exposing sensitive data when using a device from work.

Only use approved software on work devices.
For example, don't use your own app to share work-related files. Even if you're more comfortable with apps you own, security on those apps may be lacking. Have a question? Talk to the I.T. Team.

Keep software up to date on your personal electronics and home Wi-Fi network.
Open the "preferences" settings on your Wi-Fi router, the apps you use, and the operating systems of electronic devices you own. Turn on "automatic updates."

And yes, you should install antivirus on your personal computer, tablet, and smartphone.
Plus, a password manager, VPN software, and a way to back up all your files automatically. Do a web search to find reliable brands for electronic devices you use.

Lock down the Wi-Fi where you live.
Change the password that came with your Wi-Fi router and give your home network a name that doesn't identify you.

Never leave electronic devices unattended in a public place.
In the time it takes you to use a restroom, your device could be quickly compromised by a threat actor with a USB stick that types pre-programmed sequences at 1000 words per minute.

Require password or biometrics to access your phone, laptop, and tablet.
Yes, it's a minor hassle to have to enter a password, use your fingerprint, or scan your eyes every time you want to use your electronics. But if you lose the device, your data will be much safer.

Use your own cables.
Rather than plugging into a public charging station, bring your own USB battery charger. And never use a charger, USB stick, or cable you find lying about.

When in public, use a privacy screen to block the view of what's on your computer.
A privacy filter is a thin sheet of plastic customized to cover the size of your computer screen. It's engineered to prevent reading what's on the screen unless the viewer is directly in front of it.

Use a VPN on devices you own whenever you access Wi-Fi in a public place.
Many of us like to work in "third spaces" — coffee shops, bars, and cafes. But those are prime spaces for hackers to operate. Activate a VPN app on your devices whenever accessing the internet there.

Resources: Forbes, Microsoft, ProofPoint, University of Central Florida, Fortinet, Helixstorm, National Security Alliance, Touro College Illinois

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION