Work From Home

Cybersecurity Employee Guide

1

Keep a Security Mindset

Your home now doubles as a workspace. Treat it as such. Lock your screen. Watch what's visible. Don't leave sensitive info out or share your device.

2

Work Mode = Company Approved Tools Only

No personal email, chat apps, or printers. Use the apps your company allows & nothing else.

3

Always Call & Verify

If you get a weird request - even from a boss - don't trust the message! Call to confirm. Attackers spoof emails & phone calls all the time.

4

Protect Access Points

- Don't reuse passwords
- Don't let browsers store them
- Always use MFA
- Use company VPNs only
- Keep your firewall and antivirus on

5

Secure Your WIFI

- Use WPA2 or WPA3 encryption
- Hide your network name
- Use a wired connection when possible
- Use a guest network to isolate work devices from everyone else's

6

Don't Try to Be IT

You're not tech support. If something breaks or seems off, don't "Google it." Call the Help Desk.

7

Update. Backup. Repeat.

- Keep software and OS up-to-date
- Enable auto-updates
- Ask IT how your data is backed up and check that it is working regularly

Security Awareness Simply Explained

See how Wizer makes it simple to stay secure, no matter where people work.

Stay Wizer

wizer-training.com