# Working Cybersafely from Home

## Use this guidance when working remotely.

1. **Public networks vs. Home networks** Public Wi-Fi networks are risky and vulnerable to being hacked.

   When working on a public network, always use VPN software. A VPN will protect the information on your laptop and your communication across the web.

2. 1/3 of us have lost a smartphone that wasn't password-protected, so all a crook has to do to steal valuable information is power up the stolen device to access it. **Set your laptop and smartphone to require a password** after a few minutes of inactivity.

3. If you're working in a public place like a coffee shop, **use a privacy screen** on your laptop so prying eyes can't see what you're working on. And add a lock screen message whenever you're away from your computer — even if you're working from home.

4. A laptop is stolen every minute in the US, often from unattended cars in shopping center parking lots. **Keep tabs on your electronics.** Never store laptops in plain sight.

5. **Turn off Wi-Fi and Bluetooth** when you're not using them. You'll reduce the chances of being hacked and extend your battery's charge.

   Also activate the "Find My Device" setting on your laptop, smartphone and tablet to increase the odds of recovering a lost device.

6. **Don't use your personal email** (Gmail, AOL Mail, Yahoo) **for work or take sensitive files home with you**. Many popular tech apps and platforms don't offer the level of cybersecurity that are necessary for official business.

7. All the other best practices for using computers still apply when you're away from the office. **Use long passwords.** Keep the operating system, web browser and apps up to date on your laptop and smartphone.

8. Always **report suspected or actual security events** to your IT team.

Zander INSURANCE

Nationally Endorsed by

THE DAVE RAMSEY SHOW