

👋 Hi there

From charging your phone at the airport to shopping online at home, everyday activities can open the door to cyber risks if you're not careful.

In this issue, we're exploring the hidden threats in daily life and the simple habits that keep your information safe—wherever you are.

Hackers can tamper with public USB charging ports in airports, hotels, and cafes—using them to secretly install malware or steal your data.

Best practice: Skip USB ports entirely. Use AC wall outlets with your own charger and cable, bring a portable battery, or use a USB data blocker that prevents data transfer while allowing charging.

Cybercriminals often set up lookalike Wi-Fi networks in hotels, airports, and coffee shops to steal logins or spy on your activity. Even legitimate public networks can expose your data if they're not properly secured.

Best practice: Avoid logging in to sensitive accounts or entering payment details on public Wi-Fi. If you must connect, use a VPN or stick to general browsing only. Whenever possible, default to your cellular connection for safer access.

Internet-connected gadgets like smart TVs, doorbell cameras, and voice assistants can expose sensitive information if left unsecured. Many ship with weak default passwords like "admin" or "password123" that attackers can easily guess.

Best practice: Change all default passwords to strong, unique ones, and keep device software up to date. Review what data your devices can access and turn off unnecessary features that might compromise privacy.

1	V						E						
2	C											Y	
3	W		I										
4	N					K							
5	P						S						

Answers: 1. vigilance, 2. cybersecurity, 3. win, 4. network, 5. passwords



Not every defense requires advanced tools or hours of training. Some of the **most powerful cybersecurity habits are the simplest**—and they take just seconds to apply:

- **Turn on MFA (Multi-Factor Authentication)**
Even if your password is stolen, MFA blocks most unauthorized logins.
- **Use Strong, Unique Passwords**
Don't recycle the same password across accounts. A password manager can do the heavy lifting for you.
- **Lock Your Devices**
Phones and laptops hold work and personal data. Set them to auto-lock after a short period of inactivity—and never leave them unsecured in a public place.
- **Power Up Safely**
Use your own charging brick and cable instead of public USB ports.
- **Connection with Caution**
Avoid public Wi-Fi for sensitive tasks. Use a hotspot or VPN when possible.
- **Shop Smart**
Stick to trusted retailers, double-check URLs, and look for “https” before entering payment info—and only buy smart devices if you're sure they're secure.

These “low-lift” habits take almost no effort, but together they create a strong security baseline that frustrates attackers and protects you everywhere.

👉 Cybersecurity isn't just a workplace rule—it's a life skill. Every device, every network, every purchase is a chance to practice safe habits. Security goes wherever you go.

Your organization is partnering with Adaptive Security to offer you industry-leading security training.



902 Broadway, Floor 8
New York, NY 10010