U.S. AIR FORCE
Chief Information Security Office (CISO)

The office of the Chief Information Security Officer enables the US Air Force core missions — to fly, fight, and win in air, space, and cyberspace — by ensuring the cybersecurity and resiliency of systems, information and staff.

CYBERSECURITY AWAY FROM THE OFFICE

SOCIAL MEDIA

- Do not post exact location details about travel or family travel plans
- Report trolls and online abusers
- Ensure usernames & profile descriptions don't contain personally identifiable information

PASSWORDS & FINGERPRINTS

- Opt-out of saving passwords online
- Limit fingerprint access on personal devices to your own (e.g. banking)
- Do not use the same password for multiple accounts — hack one and you've hacked all!

HOME NETWORKS

- Contact your service provider to request the highest encryption configuration
- Limit devices accessing home networks to family only
- Set up open access guest networks for visitors

BLUETOOTH SAFETY

- Always change the default password
- Change settings to disable auto-pairing (includes your car!)
- Only turn on Bluetooth when connection is needed.

INTERNET SAFETY

- Enable ad-blockers on your browsers
- Disable third-party cookies via browser settings
- Install anti-spyware and anti-virus software; update regularly

PORTABLES

- Use privacy screens
- Don't leave devices unattended
- Don't automatically connect to public WIFI— use a VPN or encrypted connection if possible

PHISHING & SCAMS

- Check all URLs for accuracy before accessing any site
- Think before opening attachments
- Look out for emails with misspellings or grammatical errors

INTERNET SAFETY PRO-TIP:

Confirm there is an HTTPS on your online banking and shopping sites.

The **s** at the end of **https** marks the URL as secure. This means that the data sent between your device and the website is encrypted.

PORTABLES PRO-TIP:

Double-check privacy settings when apps on your portable devices update.

App privacy settings are defaulted to share info. Even if you've changed them, they can reset to default when updates are pushed through. Check each update's Release Notes and privacy settings to ensure you aren't unintentionally sharing information.

PHISING & SCAMS PRO-TIP:

Deleting suspicious email is good; marking it as SPAM is better.

When you mark an email as SPAM, your email provider will remember the sender and filer that sender into a SPAM folder. This decreases the chance that you will interact with scam-mers or malware.

For more information, visit: af.mil/cybersecurity.aspx