Have a Worry-Free Summer

Stay Cybersecurity Safe!

Office of Information Technology
Division of Information Security
JULY 2025

Summer is underway! As we pack up for a long vacation or a brief getaway, it's essential to stay cyber-secure.

While vacationers relax, cybercriminals continue to work around the clock, seeking every opportunity to breach security defenses. So, instead of worrying about how to stay cybersafe, let's prepare ahead of time.

Always remember that your Government Furnished Equipment (GFE) should never travel with you without prior approval and never out of the country. You must follow all of the rules for GFE that you agreed to in the IHS Rules of Behavior. ***The following tips apply to your personal electronics.***

That said, here are a few tips to ensure your summer is enjoyable and your personal electronics stay cybersecure:

Before your trip

- If traveling (nationally or internationally), review the CISA for important information and resources, including specific requirements for countries designated as high-risk or heightened-cyber-risk.
- While traveling, consider using a temporary device, such as a prepaid cell phone, especially when traveling internationally.
- Apply operating system and software application updates and download any necessary applications, such as a VPN.
- Avoid purchasing electronic cables and hardware when traveling internationally.
- Use strong passwords to prevent unauthorized access in the event of loss or theft.
- Avoid sharing travel plans on social media.

During Your Trip

- Keep all your devices secure
- Avoid using public Wi-Fi and hotspots
- Disable Wi-Fi and Bluetooth when not in use
- Avoid using public computers to log into online accounts or access sensitive data
- Avoid plugging in untrusted accessories

Staying Protected

- Enable multi-factor authentication across accounts
- Stay Updated on seasonal phishing tactics
- Set up automatic alerts for suspicious login attempts
- Review and reinforce VPN and remote access policies
- Monitor endpoints and email traffic for unusual behavior

After Your Trip

- Change any passwords used while traveling, especially internationally
- Run antivirus scans on devices used while traveling
- Monitor your online accounts for unusual activities

A Few Common Scams to Watch Out For

- Fake invoice emails posing as vendors
- "Urgent" messages appearing to come from execs who are traveling
- Travel-themed phishing campaigns
- Malware hidden in seemingly harmless email attachments

Take precautions and have a happy and safe summer!

Note: The links in this document are for informational purposes only, and do not signify an endorsement of any products contained within the linked sites/files.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.