

## Overview

We want you to be able to make the most of technology at all times, including when you travel. In this newsletter, we cover how you can connect to the Internet and use your devices securely on the road.

Mark Williams is the Enterprise Security Architect at Blue Cross Blue Shield of Tennessee. He is also a SANS instructor and President of the ISSA Chattanooga chapter. He has traveled extensively and understands the issues encountered when taking your tech toys along with you.

## Pre-check

While your network at home or at work may be secure, you should assume that any network you connect to when traveling cannot be trusted. You never know who else is on it and what they may be doing. Here are some simple steps that go a long way to protecting you and your data before you travel:

- The safest information is information you don't have. Identify what data you do not need on any devices you are bringing with you and then remove that information. This can significantly reduce the impact if your devices are lost, stolen, or impounded by customs or border security. If your trip is work related, ask your supervisor if your organization provides devices that are used specifically for working while traveling.
- Lock your mobile devices and/or laptop with a strong password or passcode. This way, if it's stolen or lost, people cannot access your information on it. In addition, enable or install full disk encryption on your mobile devices and laptops. For most mobile devices, this is automatically enabled when you use a screen lock.
- Install or enable software on your device so you can remotely track where your device is, and even remotely wipe it, if it has been lost or stolen.
- Update your devices, applications, and anti-virus software before leaving so that you are running the latest versions. Many attacks focus on systems with outdated software.





a closed padlock in your address or URL bar. In addition, you may have what is called a VPN (Virtual Private Network), which can encrypt all of your online activity when enabled. This may be issued to you by work, or you can purchase VPN capabilities for your own personal use. If you are concerned that there is no Wi-Fi you can trust, consider tethering to your smartphone. Warning: as we mentioned earlier, this can be expensive when traveling internationally. Check with your service provider first.

## Public Resources

Do not use public computers, such as those in hotel lobbies or at cyber cafes, to log in to any accounts or access sensitive information. You have no idea who used that computer before you, and they may have infected that public computer accidentally or deliberately. Whenever possible, use only devices you control and trust. At best, public computers are good for public information, such as checking the weather or catching up on the news. Signing in to any accounts, such as your Google account, could be an invitation to hackers who might be watching.

## Security Awareness Posters

Learn how to protect your family, friends, and coworkers with this series of friendly and free security awareness posters. Download the posters from <https://securingthehuman.sans.org/u/i58>.

## Resources

- Passphrases: <https://securingthehuman.sans.org/ouch/2015#april2015>
- Backups: <https://securingthehuman.sans.org/ouch/2015#august2015>
- Malware: <https://securingthehuman.sans.org/ouch/2016#march2016>
- Encryption: <https://securingthehuman.sans.org/ouch/2016#june2016>
- OUCH Archives/Translation: <https://securingthehuman.sans.org/ouch/archives>

## License

OUCH! is published by SANS Securing The Human and is distributed under the \_\_\_\_\_

\_\_\_\_\_