OUCH! | February, 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Pre-Check
- Lost/Stolen Devices
- Wi-Fi Access
- Public Resources

Staying Secure on the Road

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.

Guest Editor

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 Many attacks focus on systems with outdated software.

Staying Secure on the Road

- Do a complete backup of all your devices. This way, if something does happen to them while traveling, you still have all of your original data in a secured location.
- For international travel, check what service plan you have for your phone with your mobile service provider. Service providers often charge high rates for international data usage; you may wish to disable your cellular data capabilities while traveling internationally or purchase a local prepaid SIM card to allow for international travel.

To stay secure while traveling, secure your devices before leaving home, keep them physically secure, and encrypt all online activities.

Lost/Stolen Devices

Once you begin your travel, ensure the physical safety of your devices. For example, never leave your devices in your car where people can easily see them, as criminals may simply smash your car's window and grab anything of value they can see. While crime is definitely a risk, according to a recent Verizon study, people are 100 times more likely to lose a device than have it stolen. This means always double-check you still have your devices when you travel, such as when you clear security at the airport, leave a taxi or restaurant, check out of a hotel room, or before you disembark from your airplane. Remember to check that seat back pocket!

Wi-Fi Access

Accessing the Internet while traveling often means using public Wi-Fi access points, such as ones you find at a hotel, a local coffee shop, or the airport. There are two problems with public Wi-Fi: you are never sure who set them up and you never know who is connected to them. As such, they should be considered untrusted. In fact, this is why you took all the steps to secure your devices before you left. In addition, Wi-Fi uses radio waves, which means anyone physically near you can potentially intercept and monitor those communications. For these reasons, if you do use public Wi-Fi, you need to ensure all of your online activity is encrypted. For example, when connecting online using your browser, make sure that the websites you are visiting are encrypted. You can confirm this by looking for 'HTTPS://' and/or an image of

Staying Secure on the Road

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