OUCH! | February 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

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

Staying Secure on the Road

Overview

In this newsletter, we will cover how you can securely connect to the Internet and get things done while traveling.

Guest Editor

Steve Armstrong is the Technical Director of CyberCPR at Logically Secure, a certified SANS instructor and former course author at SANS. He is active on Twitter as **@Nebulator** and on Google Plus as **+SteveArmstrongSecurity**.

Pre-check

While your network at home or at work may be secure, you should always assume that any network you connect to when you travel is untrustworthy. You never know who else is on it and what threats they may pose. Some simple pre-travel measures can go a long way towards protecting your data while you travel. Take these precautions one or two weeks before your trip:

- Identify what data you do not need on the devices you are bringing with you and then remove any unneeded information. This can significantly help reduce the impact if your devices are lost, stolen or impounded by customs or border security staff. If your trip is work related, ask your supervisor if your organization provides alternative devices that are used specifically for working while traveling.
- For international travel, check what type of power connectors the country uses. You may need to get an adapter for charging your devices. In addition, check what service plan you have for your phone with your mobile service provider. Often, service providers charge high rates for international data usage; you may want to disable your cellular data capabilities while traveling internationally or change your service plan for international travel.
- Install 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. Many mobile devices already have this functionality built in; you may only have to enable it. (Just remember that these need Internet access to operate.)

Take these precautions one or two days before traveling:

Staying Secure on the Road

- Update your devices, applications and anti-virus software so that you are running the latest versions.
- Enable all the appropriate security settings on your device, such as your firewalls.
- Lock all of your mobile devices with a strong password or passcode. This way, if you lose your device or have it stolen, people cannot access your information on it.
- Encrypt all of your devices so that if they are lost or stolen, the data can't be accessed. Some devices, such as iPhones, do this automatically if you set a password or passcode on the device.
- Do a complete backup of all your devices. This way, you still have all of your data in a secured location if something does happen to them while traveling.

The key to staying secure while traveling is securing your devices before leaving home, keeping them physically secure, knowing where they are at all times and encrypting 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 will simply smash your car's window and grab anything of value they can see. One idea is to bring a cable lock so you can physically lock your devices, such as your laptop, when you leave them. While crime is definitely a risk, what you may not realize is that you are actually far more likely to lose your device than have it stolen. According to a ten-year Verizon study, people are 15 times more likely to lose a device than have it stolen. This means you should always double-check that 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.

Wi-Fi Access

Accessing the Internet while traveling often means using public Wi-Fi access points, such as the ones you find at a hotel, your local coffee shop or the airport. The problem with public Wi-Fi access points is not only are you never sure who set them up, but 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 to communicate from your device to the Wireless Access Point. This means anyone physically near you can potentially intercept and monitor those communications.

Staying Secure on the Road

This is why 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 the websites you are visiting are encrypted. (They will have 'https://' by the URL and an image of a closed padlock.) In addition, you may have what is called a VPN (Virtual Private Network) account, which will encrypt all of your online activity. 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 are no Wi-Fi access points 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 Computers

Do not use any public computers, such as computers in hotel lobbies, libraries or at cyber cafes. You have no idea who has used that computer before you; they may have infected that public computer accidentally or deliberately. Whenever possible, use only devices you control and trust for any online activity. If you must use a public computer, do not use any services that require you to log in or type a password.

Securing The Human Blog

Be sure to check out the STH Blog, which covers recent articles and trends on security awareness. This month, we cover the business case for Developer Training. More at http://www.securingthehuman.org/info/173952.

Resources

Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

License