

OUCH!

IN THIS ISSUE...

- Planning ahead
- Dealing with public networks
- Avoid using public computers

Staying Secure Online While Traveling

GUEST EDITOR

Raul Siles is the guest editor for the April issue of OUCH! Raul is the founder and senior security analyst with Taddong (www.taddong.com), SANS author and instructor, and security passionate (www.raulsiles.com). You can follow Raul on Twitter at @taddong and his blog at blog.taddong.com.

OVERVIEW

Going online has become universal. We expect Internet access wherever we are for whatever we need. However, when you are on the road or on vacation, accessing the Internet can be challenging. Connections may be not only slower but also at greater risk, especially when connecting to public networks or using a public computer. The key to using the Internet securely while traveling is to understand these additional risks, use caution, and be prepared.

PLANNING AHEAD

One of the most effective ways you can protect yourself when traveling is to first take simple, preventive steps before you leave.

- Update your laptop and smartphone operating systems and applications to the latest version reduce their vulnerability to attack.
- Make sure the firewall on your laptop is enabled. This helps prevent others from connecting to your laptop over the network.
- Check that your anti-virus software is up-to-date and in good working order.
- Laptops and smartphones are targets for thieves and easy to lose. Enable automatic screenlock on your laptop and smartphone using a strong password or, at the very least, a PIN code.
- Consider attaching a label with your name and email address or phone number, so that you can be

Staying Secure Online While Traveling

contacted if you lose a device, such as at airport security. Offering a reward for their safe return often helps.

- If your laptop or smartphone has personal or confidential information stored on it, consider encrypting the information or your entire hard drive before you leave. Check with your supervisor about your organization's security policies. Encryption may be required.
- If you set an out-of-the-office message at work, identify a colleague as an alternate point of contact while you are gone. In addition, do not provide specific details about your trip. If possible, limit delivery of your out-of-the-office message to recipients within your organization or to people already in your address book.
- Check with your IT department to see what special services they offer to travelers.

In addition to preparing ahead of time, there are several things you need to consider once you are traveling.

CONNECTING TO PUBLIC NETWORKS

A public network is a network to which anyone has access, such as those that are available at airports, hotels, restaurants, and cafés, usually in the form of Wi-Fi connections. When you connect to a public network, your online activities can be monitored by others. In addition, malicious individuals may operate fake Wi-Fi networks that are designed to fool you into using them and potentially attack your system.



The key to connecting online securely while traveling is to understand the risks and prepare ahead of time.

When possible, use a sponsored Wi-Fi networks hosted by a legitimate organization. Look for signs with the name of the Wi-Fi network displayed in the hotel lobby, airport terminal, or café. Using these sponsored networks is a better security bet than picking a public Wi-Fi network at random. In addition, when possible use encrypted Wi-Fi networks, and pay attention to the type of encryption. In order from best to worst, the common Wi-Fi encryption types are: WPA2, WPA, and WEP.

Even with Wi-Fi encryption, your communications could still be intercepted by other users of the same Wi-Fi network.



Staying Secure Online While Traveling

Take the additional precaution of using an encrypted data connection. The most common data encryption methods are HTTPS (SSL/TLS) and VPN (Virtual Private Network).

An HTTPS browser session, usually indicated by the familiar padlock icon, encrypts the information you send over the Web. Many websites and online services, such as Google, Gmail, Twitter, and Facebook allow you force that HTTPS encryption be used at all times.

You create a VPN by installing software on your computer that encrypts your online activities. Contact with your IT department to find out if your organization supports a VPN. If not, consider purchasing a VPN service for your personal use (<http://preview.tinyurl.com/67mnrng>).

Another option is to use your smartphone as a Wi-Fi access point. If you have a smartphone, contact your service provider about using its +3G capabilities to set up a secure “tethered connection” or “personal Wi-Fi hotspot” for your laptop. In addition, your smartphone’s email and browser capabilities may be enough to meet your needs while on the road. If so, the security afforded by your smartphone’s mobile broadband connection is a better bet than public Wi-Fi.

AVOID USING PUBLIC COMPUTERS

Public computers are those that anyone can use, and are found in libraries, hotels, and cafés. There is no way for you to know who used the computer before you. It may have been infected or otherwise compromised accidentally, or malware may have been planted on it deliberately. Any information you enter may be stolen by cybercriminals.

Limit your use of public computers to casual web browsing only, such as checking the weather, the status of your flight, or catching up on the news. If you have no choice but to use a public computer to make a transaction or to communicate sensitive information, assume that any information and your login and password you used have been compromised. Keep track of the accounts you had to access and change your passwords immediately the next time you have access to a trusted computer and network.

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at <http://www.securingthehuman.org>.

OUCH! is published by the SANS Securing The Human program and is distributed under the [Creative Commons BY-NC-ND 3.0 license](http://creativecommons.org/licenses/by-nc-nd/3.0/). Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy