Security on the Go

Because of the small size of our mobile devices, such as laptops and smart devices, we may take them for granted, not realizing that they are powerful machines, essentially, fully functional computers. With that tremendous power comes risks, and when you are out and about with these mobile devices, you need to make sure your information and devices are protected from loss, theft or compromise.

Who Would Take My Information and Why?

When it comes to crime (cyber or not), one of the main factors driving criminals is money. Our information and devices (cellular phones included) have a value for cyber criminals.

Many hackers and cyber criminals look for the easiest targets to maximize their returns. Wi-Fi networks are not as secure as the traditional wired or cellular networks, and the criminals take advantage of this. They can set up at cafés, hotels, or anywhere free and/or public Wi-Fi is provided, and capture the traffic.

Criminals may gain access to your device or information, such as through an unsecured Wi-Fi connection or picking up a lost device. Once they do, they may access your accounts, address lists, photos, and more to scam, harm or embarrass you or your friends; they may leverage stored passwords to access your bank and credit card accounts, stealing your money or making credit card charges; gaining access to sensitive material and more.

Protecting Smart Devices

Our increased reliance on smart devices – including mobile phones and tablets – for everyday activities has not gone unnoticed by cyber criminals. There has been an increase in malware and hackers targeting mobile devices in the last few years. As we do with our personal computers, we have to ensure that the proper steps are taken to protect our information and devices.

- Update the operating system. Smartphones are computing devices that need to be updated. Updates often provide you with enhanced functionality and enriched features, as well as fixes to critical security vulnerabilities.
- Password protect your device. Enable strong password protection on your device and include a timeout requiring authentication after a period of inactivity.
- Use security software. Many of these programs can locate a missing or stolen phone, back up your data, and even remotely wipe all data from the phone if it is reported stolen.
- Enable encryption. Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.
- Install and use only reputable apps provided from trusted sources. Keep these apps updated.
- Carefully review your bill to identify any unusual charges.
- Disable Bluetooth and Near Field Communication capabilities when not in use.
- Securely dispose of your device by using the "factory reset" function to remove all data from the device and return it to the condition it was in when purchased.

Protecting Your Laptops

The mobility provided by laptops also increases your risk, since you may not be protected by your organization's security or home network security. In addition, you don't know who may be on the same network if you are connected to a public Wi-Fi. Don't let security slide; secure your laptop and your information while on the go.

- Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.
- Secure your computer by enabling your firewall, as well as installing and using an anti-virus, anti-malware, and anti-spyware software. Be sure to check that any anti-virus/anti-spyware software installed is running and receiving automatic updates.
- Password protect your laptop and enable a screensaver or screen shut-off. This locks your computer and a password has to entered to re-gain access to the laptop.
- Don't leave your laptop unattended in your hotel room, at the coffee shop, or anywhere else.
- Consider purchasing a privacy screen filter if you work in crowded and busy areas and need extra privacy.
- Use encryption for your most sensitive files such as health records, tax returns and financial records. Make regular backups of all your important data.

General Security Practices

Make sure that you take the proper precautions to protect your information. This includes physical protection too – who needs to intercept your Wi-Fi or cell connection if they can just steal your device?

- Use secure wireless access when transmitting sensitive information.
- When entering sensitive or private information on a website, use a secure connection such as HTTPS, to send information, even if you are accessing the site from your cellular network.
- Encrypt your sensitive data stored on your computer and when in transit.
- Install a remote system wiper to remove your private information if your device is lost or stolen.
- Heed security warnings from your browser: if the website is considered untrusted, don't take the risk!
- If available, use a Virtual Private Network (VPN).

For More Information

- MS-ISAC Newsletters:
  www.msisac.cisecurity.org/newsletters/
- MS-ISAC Daily Tips:
  http://msisac.cisecurity.org/daily-tips/
- SANS Ouch Newsletters:
  http://www.securingthehuman.org/resources/newsletters/ouch/
- Stay Safe Online:
  http://www.staysafeonline.org/stay-safe-online/
- STOP. THINK. CONNECT – Tips and Advice:
  http://stopthinkconnect.org/tips-and-advice/

MS-ISAC

MULTI-STATE
Information Sharing & Analysis Center™

www.msisac.org
info@msisac.org
(518) 880-0686

The information in this document is provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the Center for Internet Security (CIS), for non-commerical informational and educational purposes only. CIS does not warrant the accuracy or completeness of the information or commit to issue updates or corrections to the information. CIS is not responsible for any damages resulting from use of or reliance on the information contained herein.

Smarter Online = Safer Online

Securing Your Data on the Go

Protect your private information while using smart devices, laptops and public Wi-Fi

CENTER FOR INTERNET SECURITY®

William F. Pelgrin
President and CEO
www.cisecurity.org