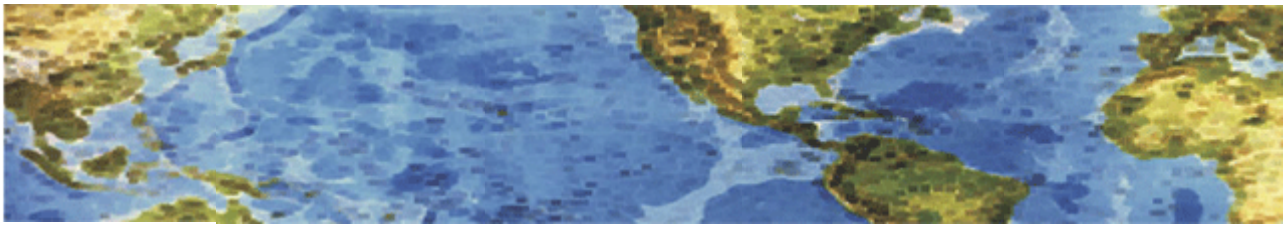
HALL ASSOCIATES



Risk-Based Decision Making Commentary
March 26 2013 Newsletter

Do You Know How to Secure Your Mobile Device?

Think about the last time you used your smartphone or tablet. Did you check your email? Track your finances? Post a photo or check in to a location? Most likely, making phone calls is just one small part of how you use your mobile phone on a daily basis. The ease and accessibility of computing from your smartphone **brings increased risks**. Everyone should follow simple tips for safeguarding our phones the same way we protect our computers and laptops.

The Federal Communications Commission (FCC) recently released Smartphone Checker designed to help the many smartphone owners who aren't protected against mobile security threats. Go to http://www.fcc.gov/smartphone-security to access the Smartphone Security Checker.

The following are simple tips to secure your mobile device:

Set PINS and passwords. You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

Do not modify your security settings. Altering your factory settings undermines the built-in security features offered by your wireless service provider and smartphone manufacture making it more susceptible to an attack.

Backup and secure your data. Backing up your data such as your contacts, documents, and photos will allow you to conveniently restore the information if it is lost, stolen, or accidently erased.

Only install apps from trusted sources. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents.

Understand app permissions before accepting them. Make sure to also check the privacy settings for each app before installing.

Install security apps that enable remote location and wiping. Visit CITA for a full list of anti-theft protection apps: http://www.ctia.org/consumer_info/safety/index.cfm/AID/12087.

Accept updates and patches to your smartphone's software. By keeping your operating system current, you reduce risk of exposure to cyber threats.

Be smart on open Wi-Fi networks. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals.

Wipe data on your old phone before you donate, resell, or recycle it. Reset the phone to its initial factory settings.

Report a stolen smartphone. The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider.

HALL ASSOCIATES

The U.S. Secret Service Electronic Crimes Task Force

In March 2012, the U.S. Secret Service, in coordination with U.S. Immigration and Customs Enforcement (ICE), arrested 19 individuals in nine states in "Operation Open Market." This was an investigation into transnational organized crime which operated on multiple cyber platforms and whose **members bought and sold stolen and personal financial information from ordinary citizens.** The group engaged in crimes such as identity theft and counterfeit credit card trafficking. This operation demonstrates how cybercrime extends beyond state lines and operates in the virtual networks and systems **that connect all of us.**

Over the years, the way we manage and spend our money has changed to include fewer cash transactions and more electronic methods, such as direct deposit, automatic payments, and online banking. Now that most financial transactions happen virtually, fraud artists to violent criminals are able to exploit technology to expand and diversify their criminal portfolio. Many crimes affecting individuals – including credit card fraud, identity theft, and embezzlement – are increasingly conducted, or at least facilitated, through the Internet.

As technology evolves, the scope of the Secret Service's mission has expanded from its original counterfeit currency investigations to include emerging financial crimes. To identify and combat electronic crimes, the Secret Service's Electronic Crimes Task Force provides a framework and collaborative crime-fighting environment that brings together federal, state, and local law enforcement, academia, and private industry. The Secret Service continues to work to provide a safer and more secure and resilient cyber environment by arresting cyber criminals.

While the Secret Service and other law enforcement professionals across the country are working hard to combat cybercrime, **emerging cyber threats require everyone, including members of the public, to take part in the shared responsibility to create a safer cyber environment.**

Below are some tips that can help you have a safer and more secure online experience.

Protect all devices that connect to the Internet. Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

Check website security. When banking and shopping, check to be sure the sites is security enabled with "https://" or "shttp://"

Beware of unsolicited email or suspicious websites. **Never** provide your credit card number, bank account information, or other personal information in response to an unsolicited e-mail or on suspicious Internet web sites.

Visit www.dhs.gov/stopthinkconnect or http://www.secretservice.gov/faq.shtml#faq11for more information.