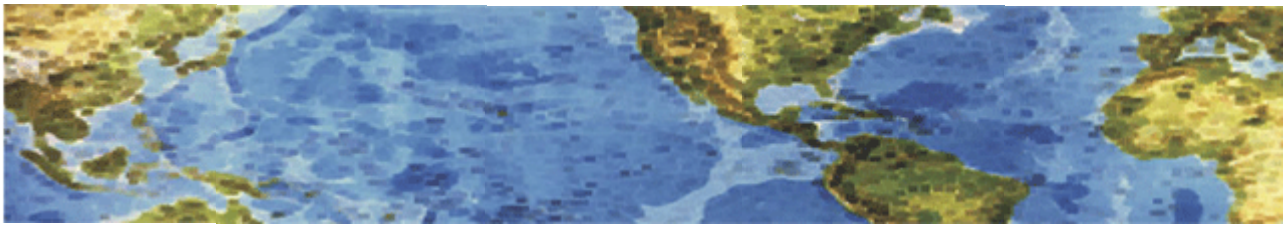
HALL ASSOCIATES



Risk-Based Decision Making Commentary
November 2012 Newsletter #2

Mobile Device Malware Risk Increases

Mobile malware (malicious software downloaded to your smart phone) is exploding at a time when financial institutions and small businesses are increasing their mobile banking offerings and consumers are making broader use of smart phones and tablets. A recent study from software and security firm Trend Micro finds that mobile malware attacks hit record numbers in the third quarter, with Android devices as the primary targets. The increase in the threat is dramatic, but traditional countermeasures being used require many more updates than is practical on handsets, or consume too much battery power - or both. Also many (most?) mobile device users are often too hasty to provide sensitive personal and financial information when prompted by an app or browser request. But the most critical area to address is technology. Security specialists say many banks and credit unions have not invested enough in malware detection and protection technologies, regardless of the channel. Might be very useful to check your financial institution's mobile security efforts as well as increase your own

Security experts and law-enforcement authorities say anything stored on a mobile device or input via mobile applications could potentially be at risk.

Malicious or potentially malicious mobile applications jumped from 25,000 to 175,000 over one quarter. Those mobile apps primarily targeted devices running Google's Android operating system, and most contained adware or spyware. Adware is often pushed to mobile users as a free software offer in exchange for consumer information. Although some adware is legitimate, hackers are using adware that morphs into spyware to collect user information for nefarious purposes. Hackers already highjack out-of-band authentication measures put in place to verify transactions initiated via online banking, as well as steal credentials and other sensitive information input via mobile-banking apps and mobile browsing.

The Federal Bureau of Investigation's Internet Crime Complaint Center issued an alert in October about newly identified spyware risks targeting Android devices. The FBI identified two new Android Trojans known as Loozfon and FinFisher. Loozfon is designed to steal mobile numbers and contact details saved in address books, while FinFisher is spyware that enables hackers to remotely control and monitor a compromised device. The aim of both Trojans: To steal or collect personal and sensitive information stored on Android devices.

Most users (***YOU!***) have not started to think about a mobile device as a computer. They don't feel that the mobile phone or tablet is something that can be compromised. Android's significant mobile market share, coupled with its openness and ***users' reluctance to proactively secure*** Android devices, has made it an easy target for cybercrime.

HALL ASSOCIATES

Are Your E-Mails Really Private – NO!

The Internet and e-mails do seem to have an anonymizing (being anonymous or private) effects on people's thoughts. From where you sit, most people are little more than a signature and a couple of hundred black words on a white field. It's a fact, or fiction, that gives many Internet users solace. Although E-mail is supposedly private and believed to be confidential, there are many ways that E-mails can be found, seen, and read -- even if you have deleted them. The real world equivalent of an email is a postcard. When you send a postcard you know that a lot of people can read it if they want to, but they're probably be too busy to bother.

And as some people have recently learned in very real and damaging ways, online anonymity is not a guarantee. Ask former CIA Director Gen. David Petraeus and his biographer Paula Broadwell, who used the tried-and-failed technique of leaving communiqués in the draft folders of email accounts. Ask the members of the hacktivist movement Anonymous, whose leaders have been outed, arrested and convicted due to their supposedly untraceable online activities. **If anything, the Internet has made the world a less anonymous place. There are more details about more people available from more places than there have ever been. And we all throw it up there willingly.**

Although an e-mail provider does not go into your account and read e-mails you send or receive, the e-mails are archived. Your activities are also logged (to some extent). If the company's records are subpoenaed, the company must turn over all records concerning your account, including e-mails received and sent. The authorities may also look at times you signed on and off from an Internet Provider or E-mail Provider. Is it possible to communicate with others online with absolute certainty that messages won't ever be found, read and traced back to you? The short answer is NO. But you can be anonymous, sort of. It all depends on who is looking for what and how much trouble you want to go through.

Don't let all this put you off sending those email postcards. They're safe enough. Email is a less secure than your telephone or normal mail, but still safe enough for most purposes. **Just don't put anything in an email (or in an e-mail attachment) that you wouldn't want to see on the evening news.**