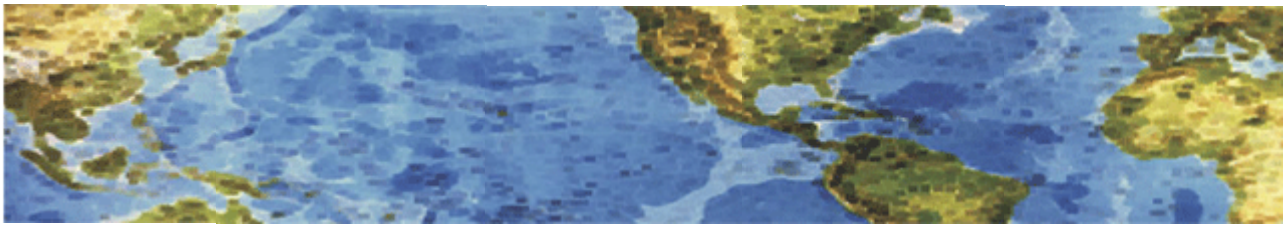
HALL ASSOCIATES



Risk-Based Decision Making Commentary
October 2012 Newsletter #1

Personal Data Theft

The confidential information of nearly 300,000 students, faculty and employees at Northwest Florida State college have been accessed by hackers in a massive security breach that happened sometime between May and September. The data accessed was in several different databases, but the hackers were able to combine all into one download. The data included names, SSNs, birthdates, bank account information for direct deposits, and other personal information.

Over 50 employees (to date) have reported issues with identity theft. Their information has been used to obtain personal loans or get credit cards. The college, local, state and federal authorities are involved in trying to locate the hackers and stop the information from being passed around the internet.

This breach shows how your information could be targeted by hackers. Does your personal and bank account information reside on somebody's server from years ago or yesterday? Have you ever provided direct deposit information to anyone at any time in your life? Do you know if their databases are protected? Have you ever requested all such information be purged or at least taken off internet accessible computers once your association with the company, college or organization was over? Do you know if the company, college or organization is encrypting and periodically assessing their systems to ensure there has not been a breach? Looks like this one was found only after some employees complained of identity theft.

Several organizations (like the credit rating companies and others) will provide a continuous web search for account numbers, SSNs and other personal information so if your information does hit the web, you can find out quickly.

HALL ASSOCIATES

Apple Device ID Targeted

Apple ID Holders have been targeted in the latest phishing scam. An Apple ID is essentially and all-access pass to an individual's Apple devices, applications and the iCloud. It allows customers to seamlessly sync their devices in order to back up and access data at home, in the office or on the road. It makes managing your online life easier – unless a scammer gets their hands on it – then seamless integrations becomes a nightmare.

This latest phishing scam targets Apple ID holders and attempts to dupe them into giving up their account information by informing them "that their Apple ID has been suspended". The e-mail usually reads:

Dear Customer, Your Apple ID has been temporarily suspended! Somebody just tried to sign in into your Apple account from another IP address. Please confirm your identity today or your account will be suspended due to concerns we have for the safety and integrity of the Apple community.

Despite the poor appearance and awkward English, the link victims are asked to follow sends them to a web page that looks almost exactly like the Apple corporate site (here would be a good place to really check the URL in the e-mail). There, users can "sign in" using their Apple ID and password. That provides these scammers enough information to access and steal personal information, data and anything else you have in your Apple devices.

All internet users are being targeted by phishing scams. Cybercriminals are on a constant (usually automated) hunt for your vulnerabilities so they can access your information. When online, everyone should be wary of sharing login information with **ANY** website, even if it appears to be a trusted one. Scammers often create dummy pages that look very familiar in the browser, but not in the address bar. So do not trust, but verify everything.