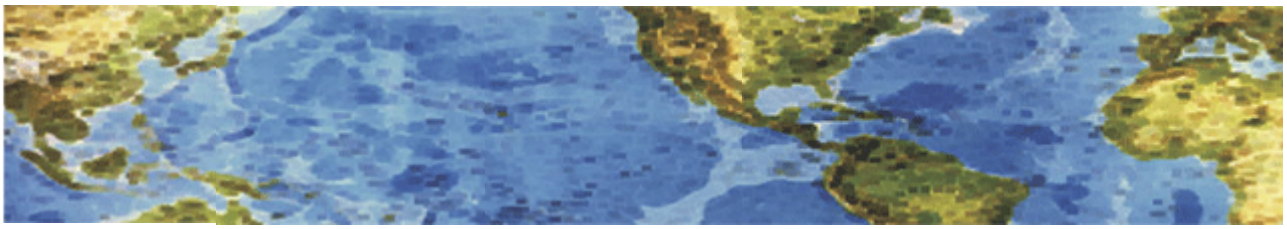
HALL ASSOCIATES



Risk-Based Decision Making Commentary
February 2013 Newsletter #1

Scammers Target Businesses With Fake E-Mails

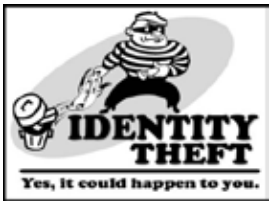
The Federal Trade Commission has issued an alert about Fake E-mail Scams. This one is for rip-off artists to pretend to represent a trustworthy and respected organization. The FTC has been hearing from businesses that have received e-mails exploiting the Federal Trade Commission name. These e-mails claim that the recipient is a target of an FTC investigation. Scammers have sent thousands of e-mails that really appear to be from the FTC. These e-mails claim that people have filed complaints about their business. So if you get an unexpected e-mail that claims to be from the FTC and asks you to click on a link or an attachment for further information about consumer complaints, DON'T OPEN IT. If you do, it will install malicious software on your computer. You can forward the e-mail to spam@uce.gov but definitely delete it. The FTC does **NOT** work complaints this way. **(www.onguardonline.gov/blog)**

Critical Safety Flaws Found in Millions of Home and Office Devices

There is a security advisory out about critical flaws in Universal Plug and Play, a networking protocol used by millions of routers, computer printers, storage drives smart TVs and lots of other devices. These flaws could let outside attackers invade your home and business network and cause havoc or steal sensitive information. Dozens of device manufacturers – including Cisco/Linksys, Netgrear, Sony, Siemens and Belkin – have been notified, but few have put out security patches yet. The US CERT advises all users to manually disable UPnP in their devices administrative settings. For that, you will have to refer to your owner's manuals or the manufacturer's websites to learn how.

The advisory is US CERT Vulnerability Note VU#922681 - Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP.

HALL ASSOCIATES



Got Money? You Are a Prime Target For Identity Thieves

Identity thieves are zeroing in on affluent individuals. (defined as those with over $1M net worth excluding family residence) . This recent phenomenon even has a specific name – Affluent Identity Theft. It turns out that the affluent aren't just at greater risks of identity theft because they have more to lose, but they are often more vulnerable as well**. However, that doesn't mean those of use less affluent or our families are being ignored.**

In most cases, the thieves who targeted these individuals are pretty well organized. They research their targets thoroughly (Do you know how much information about you is available and where it is?). This research is a combination of what is available publicly as well as gentle attacks. A gentle attack is trying to hack into your accounts, doing social engineering on you or your family/employees to find out necessary information.

There are three main reasons such individuals are being targeted:

1. They have a lot of credit and they are not good at protecting it. That is basically a mixture of being too busy and arrogance. More like "No one would dare target me. Don't they know who I am?" Or "I have lawyers to deal with that.".
2. They often have multiple accounts with high amounts on deposit, so it is much harder to protect. They normally have business accounts, brokerage accounts, investment accounts or even trust funds. So that multiplies the number of passwords needed (Of course they are all different, right?) and the subsequent protection needed. Rather than take on that task, it just gets ignored (much like all of us – you do protect your different passwords, right?)
3. There are too many points of access and vulnerability. Affluent people tend to have too many people around them – secretaries, direct employees, administrative staff, personal financial advisors, legal advisors, even family. And each one of those represents a point of vulnerability. They are people that can be exploited via social engineering.

In addition, if one of these folks becomes a victim of identity theft, they seem very hesitant to go to the authorities because of the bad publicity that would result. They just want to make it go away as soon as possible and write it off as a bad experience – something identity thieves are aware of.

There are things affluent individuals (and all of us) can do to protect themselves and their money:

1. Take the security of their identities more seriously and more personally. Don't make the mistake of assuming "it won't happen to me" or my lawyer can fix it.
2. Be very care with account information. Have a routine for updating the security of your accounts periodically.
3. Ensure that everyone around them is aware of identity security. Be wary of all calls and e-mails – think security first. Double-check everything.
4. Take precautions . Check credit reports, freeze your credit report, shred personal information, be careful with regular mail.