INFORMATION SECURITY & YOU | February 2014

Up-to-date information on privacy & preventing identity theft and financial fraud

Mobile Devices & Your Personal Information

We all ask ourselves how we would survive without our mobile devices, but we seldom ask what risks we take by using them the way we do. Whether it's for work or play, our smartphones and tablets hold a wealth of information about who we are, and we often put that information at risk without realizing it.

On an average day, we and the apps we use, access our contacts, calendar, location, credit card information, and login information to the various websites and services we have an account for. On top of that, we often post a plethora of personal information and anecdotes through social media. It's no wonder that financial fraud and identity theft continues to grow exponentially.

So how do we stay smart while using our mobile devices? Here's some guidance:

1. **Treat your device like the computer it is.** Secure it with a password, and load anti-malware apps, if available. Also, consider carefully who you lend your device to – even if it is only for a few minutes.
2. **Never save login information.** When it asks if you want it to remember your username and password, just say no! And, remember to use strong passwords.
3. **Limit across app access.** When an app asks if it can access your contacts or location, think about how that information is being used before saying yes.
4. **Don't overshare.** It's easy to go into every detail about your life on the various social media sites and apps, but a good rule of thumb is to think about who could view the posts. Remember, once it's out there, it's nearly impossible to take it back.
5. **Don't send private information via e-mail or text.** Although it's convenient, sending information like your social security number or bank account numbers is risky. Ask your bank how you can communicate with them in a secure way.

The Federal Trade Commission Makes It Easier to Talk To Your Kids About Cyber Security

The Federal Trade Commission (FTC) has recently updated their *Net Cetera* publication that guides you through topics and techniques for keeping your child safe online. Go online, and view the booklet at: *http://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf*

Social Engineering Basics – Part 1

We see it all of the time in TV shows – the clever fraudster needs to get access to a secure facility in order to download top secret information. Dressed like a company grunt, and using a bit of information gleaned from surveillance and a quick phone call, the fraudster makes it past the security desk and up to the server room in no time. The information is downloaded, and the fraudster makes a clean getaway with information that can be sold to the highest bidder.

While many think that techniques like these are made up to add drama to the show, the reality is that the methods used are pretty common, and that the information being obtained may be yours. Con artists have been using these techniques, grouped under the name social engineering, for centuries, but with the increased use of technology, fraudsters have honed their skills in order to take advantage of careless handling of customer information.

Google the words social engineering and fraud, and you will find thousands of examples of how social engineering has led to security breaches and the loss of information and money. Many of these breaches started off with a few simple actions by the con artists:

- Dumpster Diving – going through trash to find sensitive information that can be used to obtain more information.
- Pretext Calling – calling and using some basic knowledge in order to gain more information.
- Phishing – emails prompting consumers or company employees to take action that then allows fraudsters to get information or gain access to computer systems.
- Malware – computer viruses and compromised documents that load harmful code onto a computer, and can result in that computer being controlled by the fraudster

Once fraudsters have some basic information, it's often easy for them to breach the security measures of a targeted individual or organization. More and more, large scale breaches of retail and payment systems are becoming the norm as large amounts of information such as card numbers, card PINs, usernames, and passwords, can be obtained in a short period of time.

In next month's newsletter, we'll talk about some specific examples of social engineering, and how to protect your information and identity.

Identity Theft Resources

FTC ID THEFT TAKING CHARGE HOW-TO
www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

FREE ANNUAL CREDIT REPORT
annualcreditreport.com

CONSUMER REPORTING AGENCIES
Experian (*experian.com*): 1-888-397-3742
Equifax (*equifax.com*): 1-800-685-1111
Transunion (*transunion.com*): 1-800-680-7289
ChexSystems (*chexhelp.com*): 1-800-428-9623

U.S. GOVERNMENT WEBSITES
Federal Trade Commission
idtheft.gov
onguardonline.gov
Federal Reserve Bank
federalreserve.gov/consumerinfo/idtheft.htm
Federal Deposit Insurance Corporation
fdic.gov/consumers/theft
U.S. Postal Inspection Service
postalinspectors.uspis.gov

OTHER WEBSITES
National Fraud Information Center
fraud.org
American Association of Retired Persons
aarp.org
Better Business Bureau
bbb.org
Center for Democracy & Technology
cdt.org
Privacy Rights Clearinghouse
privacyrights.org

FIREWALL & VIRUS PROTECTION
(the bank does not endorse a specific product or seller, and the list does not reflect the entirety of available solutions.)
Bitdefender: *bitdefender.com*
Kaspersky: *kaspersky.com*
McAfee: *mcafee.com*
Norton: *norton.com*