A BIT ON BYTES…

Theresa Pratt
IT Manager

Periodically we have sent you information designed to help you keep your personal and financial information protected and confidential. The threats from technology that each of us face are growing and changing at a bewildering rate. We feel it is time to dedicate an entire newsletter to discussing and clarifying these issues. It is our hope you find the topics discussed here useful and helpful. Each subject is vital and something people have written volumes about. I could only touch on each briefly, so I have included links to sites where you can find more information. Stay safe!

PASSWORD SAFETY/COMPLEXITY

Passwords. We all have them and we rely on them. They guard our email, online bank accounts, online shopping profiles, iTunes accounts, and many more things. Passwords are the weakest link in our security for many reasons: we use the same word for all of our accounts, use a common dictionary word, use our children's names, pet's names or birthdate. These passwords are easy to remember, but if it is easy for us, it is also easy for a predator.

Lists are published of the most common passwords people use (see links to the right). You may be shocked to discover your password is on that list. Hackers will run through these lists trying the words against your accounts. Word to the wise: if your password appears on this list, change it now.

So what makes a good password?

- Keep the length to eight characters or more
- Substitute symbols for letters or numbers C@t@nd7h2H@t (Cat and the hat)
- Misspell a word (Superamin, B@tmyn)
- Avoid anything you can find in the dictionary (in any language)
- Avoid words spelled backwards and common abbreviations
- Don't use personal information (birthday, anniversary, driver's license number, etc…)
- Use at least one number, symbol and lower case/upper case letter
- Use a different password for each account (if one gets hacked, the rest are not vulnerable)
- Consider using a password phrase, rather than just a word, such as LuvMyShoez!!

Are you ready to put your password to the test?

- **Is your password strong enough?** www.microsoft.com/security/pc-security/password-checker.aspx
- **How long would it take for a hacker to crack your password?** www.howsecureismypassword.net

Finally, if you do use the same password for multiple accounts (i.e., your email and bank account), a danger lurks. Sites like email or Facebook tend to be more vulnerable than banking sites. Hackers therefore focus their attention on those sites. When we hear those sites have been hacked, we tend not to worry, thinking "I don't keep anything there I care about." However, the hacker now has a login name and password combination associated with you and will try it on sites you DO care about. If the combination is the same (or similar), they are in and you are hacked.

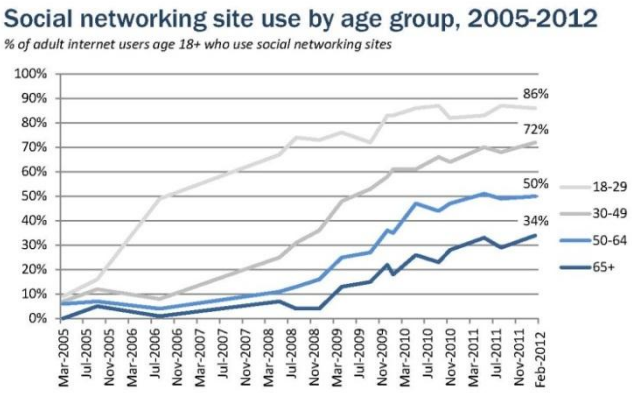
At the very least, do not use the same password for banking as you do for Facebook or email.

SOCIAL MEDIA SAFETY/RISKS/PRIVACY

Social media sites, such as Facebook, LinkedIn, Twitter, Pintrest and others are extremely popular among people from every generation. They allow us to connect with, communicate with and keep track of friends and family. We can share pictures, stories and comments with multiple people, building an online presence and community. The chart on page 2 shows how the use of these sites has grown over the past seven years across every generation.

As more and more people of every age use social media, it is important to understand the risks, particularly related to personal security and privacy.

There are two main techniques thieves use to steal your identity. They will either try to entice you to run malicious code that compromises your machine or they try to trick you into revealing personal information about yourself. Social media, by its very definition, is a place where you reveal personal information about yourself. If someone wants to find out your favorite pet's name or your mother's maiden name (read: answers to security questions), it is probably on your Facebook. Hackers understand this and target social media sites. In addition, many social media sites, especially Facebook, are set up to have everything you post available to everyone. This is a significant risk to your privacy and security.



SOME TIPS TO USE SOCIAL MEDIA SITES SAFELY

1. Use caution clicking links and liking things – any link, including the like button Facebook, can be hijacked.
2. Know what you have posted about yourself. This is a huge topic that covers subjects from your online reputation to the answers to your security questions. Follow these guidelines:
   a. Do not post anything that you would not want made public.
   b. Minimize details that identify you or your whereabouts.
   c. Keep account numbers, user names, and passwords secret.
3. Do not trust that a message requesting personal info is really from who it claims to be; confirm via alternate means.
4. Do not allow social media to scan your email address book.
5. Type the address into your browser or use a personal shortcut, rather than clicking a handily provided, and possibly hijacked link.
6. Be selective about who you accept as a friend – only friend people you know and whose identity you can verify.
7. Choose your social network carefully – not all are created equally.
8. Assume everything you post is permanent and publicly available. People have lost opportunities because of posts on Facebook.
9. Be careful with games etc. that could hijack your machine.
10. Don't use social media at work – many organizations have policies against this because of the risks described above.
11. Talk to your children about social networking. Children see the fun of social media and do not understand the risks.

FACEBOOK BREAKING NEWS

Facebook is introducing "Graph Search." This has been dubbed Facebook's biggest invasion to privacy yet. It lets users search other users profiles' for innocuous things like "my friend's favorite restaurants" or less innocuous things like "married people who like cheating date sites." A thief could search for "people who like Wells Fargo" for a list of potential targets. Protect yourself by verifying your privacy and security. Under privacy, check:

- Who can see your posts – set to friends
- Review all your posts and tags – enable
- Limit past posts – enable

Under security, check:

- Secure browsing – enable
- Login notifications – enable
- Recognized devices – validate
- Active sessions – validate

Change your Facebook password every 3 months, and double check your settings – they change.

Resource:
www.nbcnews.com/technology/technolog/consumer-reports-facebook-privacy-problems-are-rise-749990

RESOURCES TO LEARN MORE ABOUT SOCIAL NETWORKING

- http://www.microsoft.com/security/online-privacy/social-networking.aspx
- http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx
- http://blogs.msdn.com/b/securitytipstalk/archive/2010/07/08/click-fraud-cybercriminals-want-you-to-like-it.aspx
- http://blogs.msdn.com/b/securitytipstalk/archive/2010/04/07/what-is-screen-scraping.aspx

PHISHING/EMAIL SCAMS

Are you someone who cares about other people? Are you interested in finances? Are you elderly? Easily intimidated? Want to lose weight? Try to help? If you said yes to any of the above, you could be the target of a scam. Today's scammers prey on our sympathies, worries, and innate desire to help. They assume you are a good person and use that against you to steal your personal information and your resources. Phishing is a deliberate attempt by a scammer to get you to reveal information about yourself which they can use to steal from you.

RESOURCES

- http://www.onguardonline.gov/articles/0002-common-online-scams
- http://www.hoax-slayer.com/phisher-scams.html#phishing-characteristics
- http://www.us-cert.gov/nav/report_phishing.html

Scams come in all flavors ranging from work at home, weight loss, miracle cures, online dating, tech support, investment schemes and the ever popular Nigerian email scam. They are delivered as adds in the side-bars of websites, emails seeming to be from friends, calls and text messages. **Onguardonline.gov is a good resource for more information.**

There are some common characteristics of phishing to watch for:

1. Unsolicited request for information, such as a request from a bank to update your personal information.
2. Content that appears genuine, including logos that are identical to the institution they are spoofing.
3. Disguised hyperlinks and sender addresses: before clicking any link, float your mouse over it to see where it is really taking you. If the text of the link and the actual path do not match, don't click the link (see pictures of good links and bad links below for examples)
4. Clickable images – see comments above.
5. Generic greetings, such as "Dear account holder"
6. A typical ruse, such as "your account needs to be updated," "your account will be terminated", or "you received a $1,000 gift card".

This is a very broad subject. The links above will provide you with a lot of good information. **Your best protection is to remember the mantra "if it seems too good to be true, it is."**

GOOD LINK

http://www.marketstreettrust.com
Ctrl+Click to follow link
Http://www.marketstreettrust.com

BAD LINK

http://www.facebook.com/
Ctrl+Click to follow link
Http://www.marketstreettrust.com

WHAT TO DO WHEN YOU SUSPECT PHISHING

- Do not click any links.
- If it is a phone call, hang up. The longer you listen to them, the more likely they are to convince you or intimidate you into giving them personal information.
- Do not supply any personal information.
- Do not reply or contact the senders in any way.
- Do not click on any attachments.
- Report the incident to the institution that was spoofed (via alternate means than what was provided).

INTERNET SAFETY FOR CHILDREN

A former college president was quoted recently as saying "the internet is just a passing fad; therefore there is no need to invest in technology." This attitude has caused that particular college to fall significantly behind the times, and it is now having a difficult time retaining students. College students, like most children, do not believe that the internet is a passing fad. It has become the fabric on which much of their lives are built. As parents, grandparents, aunts, uncles, friends, etc. of this generation, we cannot afford to adopt this attitude. We must recognize that the internet is in fact, here to stay, and that we have a responsibility to the children in our lives to help them navigate it safely.

RESOURCES FOR PARENTS

- www.internetsafety101.org
- www.netsmartz.org/Parents
- www.safekids.com/family-contract-for-online-safety

This is a vital subject that can only be glossed over in the confines of this newsletter. Sites listed in the resources section are great tools to help you learn more. **Internet dangers generally fall into several broad categories** (taken from Internetsafety101.org)**: Pornography, predators, social networking, online gaming, cyber bullying, and mobile devices.** These categories are intertwined. You can be a part of cyber bullying via a social networking site using a mobile device, for example. The best defense we have is to **1) Get educated** and **2) Communicate openly**.

Because of the internet, pornography is only a mouse click away from your children. Statistics say that children begin consuming hard core pornography at an average age of eleven and seven out of ten teens come across porn accidentally. You should assume that your children are being pressured or encouraged by their peers to view pornography.

Predators are adults who befriend children under false pretenses with goals of abduction and sexual exploitation. They do this by "grooming" the child, or building a relationship with him or her over a period of time, gaining their trust through compliments. They take advantage of a child's natural curiosity, desire for romance or adventure, and drive a wedge between the child and his or her friends and parents, with the goal of luring them into a face to face meeting.

Online gaming presents the same concerns as internet surfing; today's game consoles have messaging and chat features. Additionally, sexual acts are often embedded in games, allowing children to engage in simulated sexual acts for "gamer points." Finally, online gaming is a hotbed for predators who pose as a child's defender or teammate.

Cyber bullying is the new version of an old problem. Historically, children could retreat to their homes and receive some shelter or break from bullying that happens at school. With cyber bullying, the bullying follows them home.

Mobile devices have introduced an entire new level of dangers to our children. With a mobile device, they have instant access to dangers including pornography, cyber bullying, predators, picture or video uploads of inappropriate or sexual content, sexting, and phone scams. They are also difficult for parents to monitor.

Basic rules of engagement are:

1) **Pay attention to what your children are doing online**
2) **Ask them non-threatening questions**
3) **Avoid overreacting when you discover something.** The goal is communication. Read the content on the Resources for Parents sites for more information.

Finally, consider an online safety contract, where you and your children discuss, agree to and sign a document outlining the rules of safe internet conduct. Safekids.com has some great templates.

As always, if you have questions or would like more information on any of these topics, please contact your wealth advisor.