The Key To Your Social Media Cyber Security: Keep The Bad Guys Guessing

PITTSBURGH, May 11, 2017 – If you've never taken the time to do an internet search on yourself, you just may be surprised about how many details of your life – past and present - are readily available to the public. Marry that information with even more personal tidbits of your daily movement or activities shared on social media channels, and you are practically handing the keys to your kingdom over to the bad guys: "Come on over and help yourself, I'm away for the day!"

> *"From teens to retirees, those with wealth to those barely scraping by, no one is immune from cyber criminals. They want what you have."*

"Social media can be a valuable tool that builds relationships and connects you to great resources for learning, and personal or business development. But, those rewards can also have risks when you volunteer information, like family relationships, geographic location and future travel plans," said Matt Darlage, director of Security Operations for The PNC Financial Services Group.

From teens to retirees, those with wealth to those barely scraping by, no one is immune from cyber criminals. They want what you have.

"If someone compromises your social media account they could potentially pose as you to friends, family, or colleagues, use available information to guess security questions, or possibly pivot to other accounts with shared passwords," said Darlage. "Depending on the information they acquire, they could open accounts in your name or make purchases, or use your reputation to gain access to networks or business accounts. All of these can result in hits to your credit score and damage to your reputation."

Protect your personal information and be more aware of your social media activity with these tips:

- **Choose smart security questions** – Your mother's maiden name? Seriously! Think of a better security question that may not be researched online. Publicly available information may include birthdates, the name of your high school, your home town, etc. How many people know your favorite color or food? Even if a bad guy tried to guess, there are so many options to choose from.

- **Boost the strength of your password** – Remember, keep the bad guys guessing; don't make it easy for them to guess your password. A strong password contains some unique combination of special characters (i.e., #, $, @, ?, !), upper-case alphabet characters, lower-case alphabet characters, and/or numbers. Avoid using simple adjacent keyboard combinations like "1234" or "abcd". And for passwords – the longer the better. This helps to put one more layer of defense between your personal information and the bad guys.

- **Do not post work-related information** – You now know to limit personal information on social media, but the same guidance applies to details about your work posted on professional networking

sites, particularly information like technology systems used, your direct reports or even your specific job responsibilities. Criminals look for information about a company's technology and a specific individual's position to find ways to infiltrate companies, often by posing as a company executive in malicious emails.

- **If you don't recognize a link, don't click it** – Has a long time professional acquaintance uncharacteristically sent you a link to a "free cruise" or video on whales they thought you might like (but you've never discussed whales)? Approach with caution. Cyber criminals are well aware that users are more likely to trust links that are sent by "friends." Unfortunately, your "friend's" account may be compromised. Reach out to the friend via another channel just to confirm the message is authentic and/or alert them to the compromise. The whale video can wait until you confirm the sender.

- **Limit "friends" or connections on social media** - If you don't know a person, it may be a good idea not to accept an invitation to connect, especially on a social media channel where you share personal or private information. Identity thieves often create fake profiles as a way to target individuals and gain information from them. Occasionally review your connections or friends to ensure you have a good idea of who is able to view what you post to social media.

- **Be careful of applications that run on social media** – Many third-party applications (apps not produced by the social media provider) can leak personal information or contain malicious software. Only install third-party applications you absolutely need and only from trusted sources.

Bottom line: Assume that whatever you post on social media could become public. If and when you do post things to social media, use available security settings wherever possible to ensure the posts are locked down to only family or friends, and never set to "public." Most reputable social media sites give you ways to protect your privacy from prying eyes. You should take full advantage of all such capabilities. At a minimum, remove any personal information such as birthday, maiden name, phone number and address. Set all photographs to friends/family only and limit personal postings to only friends and family. Lastly, sort followers and friends into proper access groups.

For more information on identity theft, visit the Security and Privacy website on www.pnc.com.

The PNC Financial Services Group, Inc. is one of the largest diversified financial services institutions in the United States, organized around its customers and communities for strong relationships and local delivery of retail and business banking including a full range of lending products; specialized services for corporations and government entities, including corporate banking, real estate finance and asset-based lending; wealth management and asset management. For information about PNC, visit www.pnc.com.

CONTACT:
Saul Boscan

(412) 762-1535
saul.boscan@pnc.com

Additional assets available online: Video (1)

https://pnc.mediaroom.com/2017-05-11-The-Key-To-Your-Social-Media-Cyber-Security-Keep-The-Bad-Guys-Guessing