Information Security E-newsletter

June 2021 | Issue 21.05

BankOnITUSA®
It's Not IT, It's IQ

TMI 4 Ur BFF?

We're all sharing more personal information than ever. On Facebook. On Instagram. Even on LinkedIn. But when is posting personal information posting too much information?

Sophisticated spear phishing attacks (attacks directed toward specific individuals) are occurring much more frequently, and they are targeting bank employees.

Names of family members, pet names, birthdays (all too frequently chosen as part of passwords) along with information such as where you went to school, travel plans, and other personal details are gathered by cyber-attackers to craft personalized emails that are specific to you.

When a cyber-attacker uses your name in an email, mentions information that is personal to you, and focuses on your likes or dislikes they are using a form of social engineering to put you at ease, causing you to let your guard down so that you will open a malware laden attachment or click on a malicious link.

Similarly, your colleagues might be more likely to click when the sender seems to demonstrate that they know you, in an email directed to them.

Here are some quick tips to consider when posting on social media sites:

- Stop and think. Then think again. Before posting ask yourself if the information is too personal and how could it be used against you.
- Consider everything you post online as being available to everyone. Forever.
- Review previous posts. Is there something you posted last week or last month that now seems too personal? Remove it. While everything posted online is forever, removing will make posts harder to find and less visible.
- Use your work email only for work, and use a personal email account for personal items
    - Pro Tip – Use a third email account for only social media purposes.
- Received a friend or connect request? Vet the account before accepting the invitation. Cyber-attackers are creating fake online profiles for you to accept and then entice you to click links that lead to malware.
- Searching for a job? Vet the company you are applying through; does the offer seem too good to be true; is the salary being offered far above market wages; is there a sense of urgency by the recruiter to fill out an employment application (employment applications contain a lot of personal data which can be used for identity theft).
- Looking for love? Dating sites are another source cyber-attackers use to get personal information and gain your trust. While you may be looking for your soulmate, the intentions of others may not be pure of heart. On some dating sites, automated bots have been uncovered meaning the person you are communicating with is not a person at all but instead artificial intelligence that is designed to capture not only your heart but also your money.

Be aware of the risks created when posting on Social media and when too much information (TMI) is too much.

Disclaimer: This publication attempts to provide timely and accurate information concerning the subjects discussed. It is furnished with the understanding that it does not provide legal or other professional services. If legal or other expert assistance is required, the services of a qualified professional should be obtained.