Paramount to asking WHAT'S in your wallet – WHO's in your wallet,

and your bank account, financial records, medical records, social security …

By: Thomas Carroll, Banking Officer & IT Administrator Covenant Bank, Summer 2017

We all enjoy today's technology and the ease, convenience and efficiency it offers. It is hard to imagine being unplugged for even a few hours let alone being decimated by a cyber incident that causes major disruption. On a personal level, a 20- year credit rating can go awry in less than 20 days. For businesses a complete shutdown could result in customer interruption and loss of revenue that necessitate a tedious, time-consuming disaster recovery process to correct.

Opinion leaders on Forbes Technology Council believe Cybersecurity should be the biggest concern of 2017; and according to INTERNET SAFETY 101, "The White House has declared identity theft as the fastest growing crime in America." As reported by SONICWALL, there are more than 6 billion phishing emails sent world-wide each month with the loss to each person successfully phished averaging $1200 (according to the Federal Trade Commission).

If these opinions, facts, and statistics have you concerned take heart, there are some ways to help prevent them. One of the best ways is to participate in security awareness training readily available – you guessed it – online. Many businesses are using these resources to provide training through multiple modules using interactive videos and games to make it more interesting. Internal IT professionals within companies are also getting more proactive in regularly communicating helpful hints to staff along with warning about current schemes and threats.

To keep your "wallet of information" safe, here are a few FAST FACTS as well as a Social Engineering Red Flags summary for email security click here for pdf

- Follow prescribed cautionary steps when opening emails
- Create strong, long, and multiple passwords for different things
- Use a variety of passwords for different things
- Be cautious of public Wi-Fi access points
- Keep Anti-Virus software and operating systems up to date
- Pay attention to suspicious activity alerts
- Avoid clicking through Pop Up screens when browsing the internet
- Inform your provider / IT department of suspected hacking activity and follow through with their instructions

To read more of our Blogs, click here