Mobile Banking App is HERE!

UNION BANK

JUNE 2019 Issue 6

SMARTPHONE SECURITY TIPS

In the 21st century, smartphones have become somewhat of a necessity. Businesses, schools and many other types of organizations require smartphones to complete daily tasks. With the users getting younger and the technology getting smarter, it is difficult to escape this new world of smart technology that we are living in. Almost anything you can think of is connected to the World Wide Web. Our smartphones are more than just a device to make a call or send an email. They are our debit cards, our entertainment, our books, calendars, and our music; and with technology advancing at the current speed, they will become much, much more.

Smartphones are just as powerful as desktops or laptops and need to be kept just as safe, or even more so because of their exposure. Since your smartphone travels with you everywhere, it is prone to be misplaced, stolen or hacked, putting you at an extremely high risk for a data breach. This is particularly important when younger kids and teenagers use these devices and are not as cautious as some adults may be. It has been reported that one in 10 smartphone owners in the United States have had their phone stolen and that number continues to increase.

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Hackers have been fans of smartphones because of the security gaps. They may not be able to target many users at the same time as they can with a network attack, but the impact can be just as damaging. Hackers are also fully aware that there is a much younger generation on these devices on a constant basis and they may be easier to target. Smartphones contain very sensitive information, especially if used for work purposes. Hackers have been able to expose many flaws and vulnerabilities in smartphones, USB sticks and SIM cards. They have even been able to penetrate through SMS texting (also known as smishing, a form of a phishing attack). Some attacks have also taken control of a smartphone's camera, microphone and GPS while stealing the user's personal information and listening to phone calls. Smartphone manufacturers and security firms are constantly trying hard to find the flaws before the cybercriminals do.

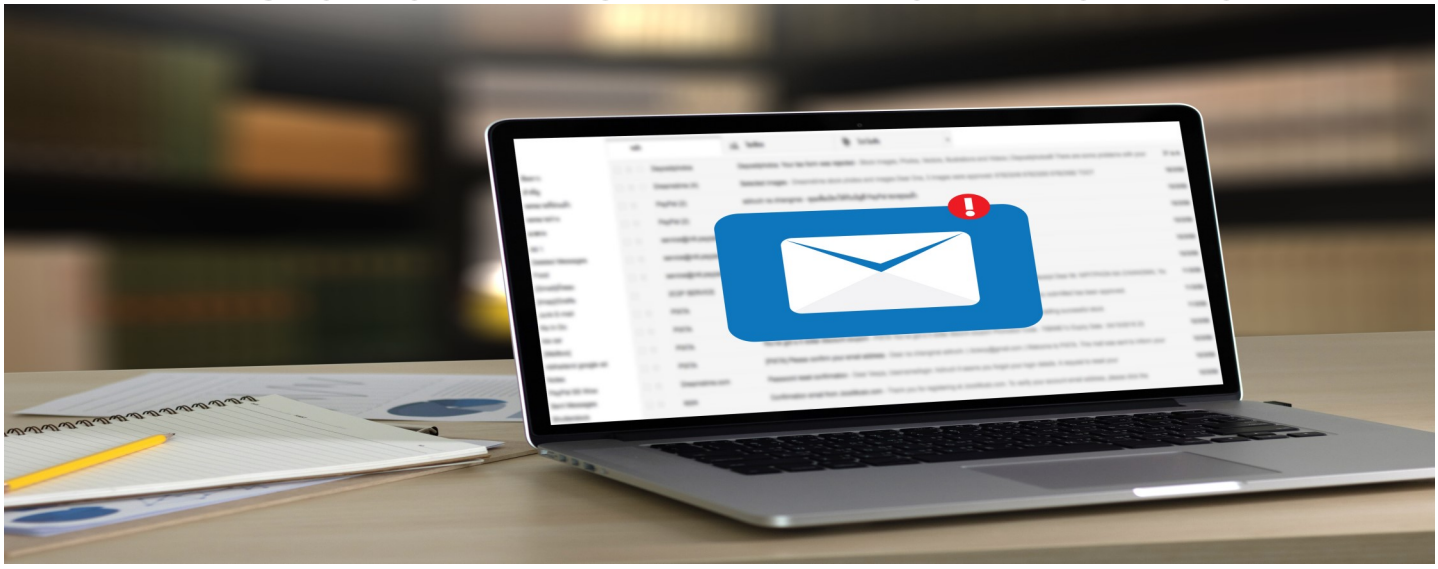
Below are some tips that will help protect you from becoming the next victim of smartphone hack:

- Secure your phone. Use a strong passcode to lock your phone. Don't use common words, birthdays or any personal information.
- Turn off Geotagging. Many phones have as a default embedded location tags. Make sure that feature is turned off.
- Don't keep your Bluetooth connection on. Hackers can access your connection if they are in range. Any unknown requests through a Bluetooth connection should ALWAYS be ignored or declined.
- Always switch off a wireless connection when it's not in use. This will ensure that malicious parties can't connect to your device without your knowledge.
- Parents should constantly monitor children's smartphones.
- Delete any text messages or emails that contain sensitive information. It is always best never to disclose sensitive, personal information about yourself via a text message or email. Sensitive personal information can include your driver's license number, social security number, password, and account numbers.
- Malware (viruses and Trojans) and fraudulent applications are out there. Only download mobile applications from authorized application stores like the Apple App Store or the Android Market.
- Keep security software current. Having the latest mobile security software, web browser, and operating system are the best defenses against viruses, malware and other online threats.
- When in doubt, don't respond. Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or for immediate action are almost always a scam.
- Pay attention to the activity of your smartphone. If you notice apps opening by themselves, if the battery drains much faster than normal or if you notice unusual charges on your wireless bill, those are signs that indicate your phone may be compromised.

Let's face it: smartphones are an important part of our lives, especially for parents and employees who are on the go and need to stay connected to kids and co-workers. But attacks on smartphones will continue to increase. Hackers are constantly looking for any chance to steal and misuse data. Taking basic precautionary measures can help protect your smartphone and all the data it contains.

Sources:
http://techlife.samsung.com/keep-smartphone-being-hacked-1067.html
http://www.computerworld.com/article/2488450/mobile-security/how-to-keep-your-smartphone–and-its-data–secure.html
https://www.digitalunite.com/technology-guides/smartphones-tablets/smartphones/10-top-tips-smartphone-security

WHAT IS CEO FRAUD AND HOW TO AVOID IT



It is unfortunate, but sometimes the weakest link in any organization could be an unaware employee. Most of the time, these are common mistakes with no malicious intent, but ones that can have significant consequences, nonetheless. Cyber attackers have learned that exploiting unaware employees can sometimes have the biggest payoff. However, knowledgeable people can also be an organization's best defense.

CEO Fraud, also known as Business Email Compromise (BEC), is not new. In these attacks, a cybercriminal pretends to be a CEO or other senior executive from within an organization. The criminals send an email to staff members that try to trick them into doing something they should not do. These types of attacks are extremely effective because the cyber criminals do their research. They search an organization's website for information, such as where it is located, who the executives are, and other organizations the target works with. The cyber criminals then learn everything they can about the organization's coworkers on sites like LinkedIn, Facebook, or Twitter. Once they know the organization's structure, they begin to research and target specific employees, picking targets based on their specific goals. If the cyber criminals are looking for money, they may target staff in the accounts payable department; if they are looking for tax information, they may target human resources; if they want access to database servers, they could target someone in IT.

Cyber criminals are sneaky—they are constantly coming up with new ways to get what they want. Once the criminals determine what they want and whom they will target, they begin crafting their attack. Most often, they use spear phishing. Phishing is when an attacker sends an email to millions of people with the goal of tricking them into doing something; for example, opening an infected attachment or visiting a malicious website. Spear phishing is similar to phishing; however, instead of sending a generic email to millions of people, they send a custom email targeting a very small, select number of people. These spear phishing emails are extremely realistic looking and hard to detect. They often appear to come from someone you know or work with, such as a fellow employee or perhaps even a manager or higher up.

The emails may use the same jargon your coworkers use; they may use an organization's logo or even the official signature of an executive. These emails often create a tremendous sense of urgency, demanding immediate action and discretion.

A successful execution of a BEC scam creates a significant burden for the both the company and the employee involved and can be very costly. So how do you protect yourself and your organization? Educating employees about the dangers of these types of attacks and using common sense is the best defense. If an employee receives a message from a supervisor or a colleague and it does not sound or feel right, it may be an attack. Clues can include a tremendous sense of urgency, a signature that does not seem right, a certain tone you would never expect, misspellings or the name used in the email being different from what the person actually calls you. The attacker may even use an email address or phone number you have never seen before, or an email address that is similar to the legitimate email. When in doubt, call the person at a trusted phone number or meet them in person (don't reply via email) and confirm if they sent the email.

Every organization may have policies that define proper procedures for authorizing the transfer of funds or the release of confidential information and those processes should never be bypassed. If a request to do something outside normal procedure is received, regardless of the source, it should be considered suspicious and be verified immediately before any action is taken. When in doubt always contact a supervisor, the help desk, or information security team right away.

The reality is every day new threats arise and evolve and organizations must always try to stay one step ahead. Having a combination of employee cybersecurity training and best practices against email threats as well as security technologies that can help users and organizations detect them is a good way to help protect any organization from these types of attacks.

Sources:
https://venturebeat.com/2016/09/19/6-critical-steps-to-avoid-ceo-fraudnow/
https://www.knowbe4.com/ceo-fraud
https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)