First Bank
& Trust Company
Member FDIC

Volume 4, Issue 7

July 2018

INSIDE THIS ISSUE:

Member FDIC
EQUAL HOUSING LENDER

Abingdon Virginia, East
276-628-3838

Abingdon Virginia, West
276-628-9558

Bridgewater Virginia
540-828-2020

Bristol Virginia, East
276-466-9222

Bristol Virginia, West
276-669-1122

Bristol Tennessee, Volunteer Pkwy
423-652-2022

Christiansburg Virginia
540-260-9060

Fairlawn Virginia
540-633-3793

Gray Tennessee
423-467-9966

Harrisonburg Virginia
540-434-0671

Johnson City Tennessee
423-975-9900

Kingsport Tennessee
423-246-3700

Lebanon Virginia, East
276-889-3401

Lebanon Virginia, West
276-889-4622

Lynchburg Virginia
434-455-0888

Norton Virginia
276-679-7401

Staunton Virginia
540-885-8000

Verona Virginia
540-248-7700

Waynesboro Virginia
540-943-5020

Wise Virginia
276-328-3439

Wytheville Virginia
276-228-1125

# Securing Your Mobile Device

## Why locking your phone is a must

There are a number of advantages to having mobile devices. Having access is a tremendous benefit in a digital world. But do we truly understand the importance of protecting that access and those mobile devices? Even after hearing stories of individuals who get their phones hacked or have their information stolen, is the seriousness of a misplaced or stolen device really something we think about after the fact? Are the necessary precautions taken to make sure we're not the next victim? Aside from making sure our operating systems and antivirus are current, and not clicking on questionable links, what other steps are we taking to help prevent an attack?

Another very easy, but crucial, step we can take is simply locking our devices. Astoundingly, most mobile users, however, do not take even this very simple step to make sure their devices are secure. Based on a 2013 study, only 27% of mobile users had a PIN or access code to get in to their phones. There was a recent story in a blog where a user (let's call him Joe) described going to an event and leaving his phone on a seat. Joe didn't realize the phone was not in his possession until he was home. At first, the realization of misplacing his phone seemed irrelevant, but as Joe called the location to verify if a phone had been turned in and hearing the answer "no, a phone has not been turned in," a sense of terror arose. Doing a quick mental check of what was stored on his phone (personal family pictures, banking apps, passwords, upcoming calendar events, email accounts, personal and work related documents), Joe quickly realized the seriousness of the situation, especially since his phone was not locked or password-protected. Fortunately for Joe, a good Samaritan did locate the phone and turned it in. But statistics show that even good Samaritans who find lost phones do a little snooping before trying to locate the device's owner. In 2012, Symantec conducted a survey that showed 96 percent of people who came a across a lost phone went through its contents.

Personal data is like monetary currency for cybercriminals. We need to treat our mobile devices the same as our laptops and computers. With new advancements like biometric authentication, it is now easier than ever to protect mobile devices. Below are just a few tips that can help.

⇒ The obvious, lock your phone using pin codes or biometric options that many new mobile devices offer.
⇒ Enable two step verification.
⇒ Encrypt your private data in the cloud.
⇒ Customize your phone to make it harder to use.
⇒ Make sure updates and upgrades are done.
⇒ Review your app permissions.

Locking your mobile devices may not always prevent a hacker from doing their bad deeds. But in the event that your device is lost or stolen, the password protection provides a road block and buys a little time for you to contact your mobile device carrier to take the next necessary steps.

*Sources:*
*https://www.computerworld.com/article/2497183/mobile-security/mobile-phone-security-no-brainer--use-a-device-passcode.html*
*ttps://www.pcworld.com/article/262216/why_locking_your_mobile_device_with_a_fingerprint_is_a_great_idea.html*

# Cybersecurity Insurance

Cybersecurity insurance is fairly new but still worth discussing. It is a complex concept and entails many different facets, but according to experts, if your company has customer or vendor relationships and processes customer-sensitive (nonpublic) information, then cyber insurance is a must.

Many organizations have been breached, sometimes unbeknownst to them. However, not all of these breaches were mass infiltration of personal data or loss of money, and most average citizens would never have known a breach even took place. Nevertheless, this does show that these particular systems were vulnerable and that an attacker was able to penetrate the company's security protocols.

Let's imagine for a moment that a cyber-criminal was able to gain access to all your customers' profiles, credit card numbers, banking information and social security numbers. Then imagine that all your company's most valuable information, like trade secrets, are now exposed and, worst yet, even held for ransom. The financial damages that could result in a worst-case scenario like this would be crippling and the aftermath of trying to regain public trust would be even worse. That's why most experts believe that cyber insurance should be at least considered when reviewing a company's IT security budget. Data breaches are a serious issue and some states are taking notice. For example, New York State Department of Financial Services has implemented regulations that require banks and financial institutions operating in that state to put in place cybersecurity programs and they must be notified of any breaches or cybersecurity event.

Cybersecurity insurance is designed to help mitigate losses during a cyber breach incident. Cybersecurity insurance covers a broad spectrum of losses and expenses. It is not a one-size-fits-all policy and companies need to look at their business' needs and how to protect their customers and assets. The truth is, cyber-attacks are becoming more common and some believe it's no longer a matter of "if" it happens, but "when" it happens. Every cyber-security strategy must have a contingency plan for when defenses are breached – and many are adamant that the contingency should now include cyber insurance.

Ultimately, organizations need to make the best decisions, not only for their bottom line but also for their customers to ensure their information is being protected and is safe from malicious attacks. It is worth at least investigating the pros and cons of the different cybersecurity policies available and how it can protect organizations. We don't know what the future holds and if cybersecurity insurance may become mandatory, but it would be beneficial to be ahead of the game and knowledgeable about the ins and outs of this product.

*Sources:*
*https://www.bankinfosecurity.com/cyber-insurance-expectations-for-banks-a-7673*
*https://bankingjournal.aba.com/2018/05/understanding-coverage-options-for-cyber-threats/*