Volume 4, Issue 8

August 2018

First Bank & Trust Company
Member FDIC

INSIDE THIS ISSUE:

Social Networking– How to Stay Connected Safely 1-2

The True Cost of Cyber Crimes on Community Banks 2-3

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

SOCIAL NETWORKING

How to Stay Connected Safely

Social networking sites such as Facebook, Twitter, Google+, Pinterest and LinkedIn are powerful, allowing you to meet, interact and share with people around the world. However, with all these capabilities come risks; not to just you, but your family, friends and employer.

A common concern about social networking sites is privacy, protecting your personal information, and the sensitive information of others. Potential dangers include:

- ***Impacting Your Future:*** Many organizations search social networking sites as part of background checks. Embarrassing or incriminating posts, no matter how old, can prevent you from getting hired or promoted. In addition, many universities conduct similar checks for new student applications.
- ***Attacks Against You:*** Cybercriminals can harvest your personal information and use it for attacks against you. These attacks can spill into the physical world, such as identifying where you work or live.
- ***Harming Your Employer:*** Criminals or competitors can use any sensitive information you post about your organization against your employer. In addition, your posts can potentially cause reputational harm for your organization.

The best protection is to limit the information you post. Yes, privacy options can provide some protection; however, keep in mind that privacy options are often confusing and can change frequently without you knowing. What you thought was private could become public for a variety of reasons. In addition, the privacy of your information is only as secure as the people you share it with. The more friends or contacts you share private information with, the more likely that information will become public. Ultimately, the best way to protect your privacy is to follow this rule: ***if you do not want your mother or boss to see your post, you most likely should not post it.***

Also, be aware of what information friends are posting about you. It can be just as damaging If they post private information or embarrassing photos of you. Make sure your friends understand what they can or cannot post about you. If they post something you are not comfortable with, ask them to take it down. At the same time, be respectful of what you post about others.

In addition to privacy concerns, social networking sites can be used by cybercriminals to attack you or your devices. Here are some steps to protect yourself:

Password: Protect your social networking account with a strong password and do not share this password with anyone or re-use it for other sites. In addition, some social networking sites support stronger authentication, such as two-step verification. Enable stronger authentication methods whenever possible.

Continue page 2

Encryption: Many social networking sites allow you to use encryption called HTTPS to secure your connection to the site. Some sites like Twitter and Google+ have this enabled by default, while other sites require you to manually enable HTTPS via account settings. Whenever possible use HTTPS.

Email: Be suspicious of emails that claim to come from a social networking site; these can easily be spoofed attacks sent by cybercriminals. The safest way to reply to such messages is to log in to the website directly, perhaps from a saved bookmark, and check any messages or notifications using the website.

Malicious Links/Scams: Be cautious of suspicious links or potential scams posted on social networking sites.

Cybercriminals can post malicious links and if you click on them, they take you to websites that attempt to infect your computer. In addition, just because a message is posted by a friend does not mean it is from them, as their account may have been compromised. If a family member or friend has posted an odd message you cannot verify (such as they have been robbed and need you to send money), call them to confirm the message.

Apps: Some social networking sites give you the ability to add or install third-party applications, such as games. Keep in mind there is little or no quality control or review of these applications; they may have full access to your account and private information. Only install apps that you need, that are from well-known, trusted sites, and remove them when you no longer need them.

Social networking sites are a powerful and fun way to communicate with the world. If you follow the tips outlined here, you should be able to enjoy a much safer online experience. For more information on how to use social networking sites safely or report unauthorized activity, be sure to review the security pages of the sites you are using.

Sources:
https://turbofuture.com/internet/The-Dangers-of-Social-Networking-Why-you-need-to-be-careful
https://www.reputationdefender.com/blog/privacy/consequences-oversharing-social-networks

THE TRUE COST OF CYBER CRIME ON COMMUNITY BANKS

Community banks have been the financial foundation for many small towns throughout the United States, and when they are victimized by a cyber attack, the cost can be enormous. All types of vulnerabilities have the potential to cause major damage. Financial institutions rank fifth among the top ten industries for targeted attacks. We commonly relate losses to what has been stolen, but seem to forget the internal cost that also affects the banks.

Long ago when someone physically robbed a bank, law enforcement was able to narrow down the potential suspects to maybe a handful of individuals. Now when dealing with a digital thief, they can basically be looking at anyone on the planet with access to a computer as a potential suspect. Here is where a bank's expenses start to add up. Between investigations, potential civil and legal claims, regulatory fines and public relations costs, a bank can spend millions just trying to catch a cybercriminal.

In 2013, McAfee sponsored a study to show the economic impact of cybercrimes on the global economy. It showed that the annual global loss is about $300 billion to $1 trillion and an estimated 500 thousand jobs were lost each year. Over the past five years these statistics have increased. The average number of breaches per company has more than tripled from 40 in 2012 to 125 in 2017.

Continue page 3

The greatest impact of cyber breaches on financial services firms are business disruption and information loss. Together this accounts for 87 percent of the cost to respond to cyber crime incidents according to the *Cost of Cyber Crime: Financial Services* which was published earlier this year.

Then there is reputational damage. Most companies spend years building a trusted brand, especially banks. But with just one key stroke by a cybercriminal they can change how customers and potential customers feel about an organization, possibly causing more monetary damages. But most importantly, the perception of the organization in the community can have lasting effects.

But community banks are fighting back. They understand that the stakes are high and are investing in creative ways to protect their customers, their institution and their communities. They are making sure their disaster recovery plans and defense mechanisms are strong allowing them to recover quickly from unplanned attacks.

The reality is cyber attacks are not going anywhere and each one may be more ferocious than the last, but community banks are armed with more knowledge and tools to help them mitigate potential damage and can better arm themselves now and in the future.

Sources:
https://www.americanbanker.com/news/ransomware-is-taking-a-toll-on-banks-heres-how-theyre-fighting-back
https://www.bostonglobe.com/business/2016/03/24/small-banks-face-greatest-risk-from-cyber-hackers/ptIWlWZh9ldFlbBxyQfx1K/story.html
https://www.slideshare.net/accenture/cost-of-cyber-crime-financial-services-87930580
https://www.insurancejournal.com/news/national/2018/02/15/480708.htm