First Bank & Trust Company
The Bank That Puts You First
Member FDIC

Volume 4, Issue 1

January 2018

INSIDE THIS ISSUE:

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

Five Cyber Security Trends of 2017 and What to Look Forward to in 2018

It's a new year! And as predicted by many experts in the cyber security field, breaches were one of the top issues facing many corporations in 2017. Along with ransomware, phishing attacks were big hits for cyber criminals in 2017. As we start off 2018, let's take a look at some of the security highlights of last year.

1. **Education is everything.** The saying that "knowledge is power" is absolutely true when talking about cybersecurity. Companies across all sectors realized more than ever before that your first line of defense against any cyberattack is a knowledgeable employee. Clicking on the wrong link or opening the wrong attachment can have detrimental impact on any corporation. Protecting a network is no longer just the responsibility of the IT team, but of everyone who has legitimate access to that network. In 2017, many companies put more time and money into educating staff in hopes of preventing the next catastrophic event.
2. **Security budgets increased.** In light of many high profile breaches, companies took a hard look at budgets and decided that it was worth putting a little extra money into cyber security protections.
3. **Companies realized Disaster Recovery Plans are no longer optional.** Hurricanes Maria and Irma proved to everyone that you can never be too prepared for anything. In September of 2017, the United States suffered two of the strongest storms ever recorded in their history. Many of those hit by those disasters are still recovering. The benefits of a DR plan are undeniable and moved to the top of the priority lists for many organizations. Although predicting a major disaster is impossible, with a DR plan in place, it may be possible to lessen some of the loss of data and services that may have a major impact on customers, employees and the business itself.
4. **Patches are extremely important.** Patches are one of the most important cybersecurity tools to help protect against malware and viruses. WannaCry is a good example of how a malware can expose vulnerabilities that were not patched.
5. **Passwords alone just didn't cut it.** In 2017, many realized that just having a password was no longer enough to protect sensitive data. Advancing technology meant methods of securing information needed to be just as progressive as the tactics cybercriminals used. Many organizations decided to implement two-step verification also known as two-factor authentication, TFA or 2FA. The extra layer of security that requires not only a user name and password, but also an additional piece of information that only the user would know, helped to ward off attacks. Although not foolproof, it made it harder for a cybercriminal to gain access to users' accounts.

Each year the technology changes and cybercriminals get more creative and flexible with their methods of attack. In 2018 many are predicting that more foreign state-sponsored attacks will increase. In light of the 2016 government hacking events, experts believe the attempts will become bolder and push limits never seen before. Also, ransomware is not going anywhere. Cybercriminals are going to take advantage of the monetary value data has and will exploit it in more sophisticated ways, such as the way they did with the Equifax breach. As each year passes, the threats become more realistic and more targeted. Do not be complacent in 2018. If you thought you have seen it all, experts are saying we haven't seen anything yet!

Sources:

https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

https://thestack.com/security/2017/12/18/cybersecurity-in-2018-what-we-can-expect-to-face/

Volume 4, Issue 1

Start the Year with a clean email account!

As we start the new year, it’s time to get rid of the old and bring in the new! Many of us have unsolicited emails clogging up our email accounts. The worst thing to see when you open up your Outlook, Gmail or Yahoo! account is hundreds and hundreds of spam emails. They are unwanted, unwarranted and just downright annoying. But the even bigger issue is that spam can become a security risk to you and your PC or mobile device. Take some time to go through your email accounts and start the year off right!

Here are some best practices to help you wade through that electronic junk:

1. Use your junk mail email filter. Microsoft office provides a filter that automatically evaluates in-coming messages and sends those identified as spam to the Junk E-mail folder. Most free email providers also have the same option.

2. If you are using Microsoft Office, turn off read and delivery receipts and automatic processing of meeting requests. Spammers sometimes resort to sending meeting requests and messages that include requests for read and delivery receipts. Responding to such meeting requests and read receipts might help spammers verify your e-mail address.

3. Limit the places where you post your email and your email address to others.

4. Yes chain emails still exist. Don't forward chain email messages. By forwarding a chain email message, you might be furthering a hoax and at the same time exposing your email address to others.

5. DON’T ever reply to spam emails, not even to unsubscribe from a mailing list, unless you know with all certainty the sender is a trusted source.

6. When shopping online, watch out for check boxes that are preselected. Companies sometimes add a check box that is already selected, which indicates that you give the company permission to sell or give your e-mail address to other businesses (or "third parties"). Clear this check box so that your email address is not shared.

7. Always be careful when giving to charity via an email request. Unfortunately, some spammers prey on your goodwill. If you receive an email appeal from a charity, treat it as spam. If the charity is one that you want to support, locate their telephone number or website to find out how you can make a contribution.

Unfortunately, we will never be able to get rid of all spam; it’s just the nature of the beast when living in a digital society. However, the tips above can help mitigate exposure to crooks who want nothing more than to wreak havoc on innocent victims.

Take some time to go through your email accounts and start the year off with a clean inbox. Try to always stay one step ahead by being vigilant and prepared!

> *“Always be careful when giving to charity via an email request. Unfortunately, some spammers prey on your goodwill.”*

Sources:
https://www.computerhope.com/tips/tip88.htm
https://www.americanexpress.com/us/small-business/openforum/articles/7-ways-to-get-rid-of-spam-forever/