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

Volume 5, Issue 1

January 2019

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

Operations Center
276-623-2265

What Experts Predict for 2019

A new year is here and many experts believe that hacking will continue to be prominent in 2019. But although cyber-criminals continue to advance their techniques, they tend to stick to that age old adage: "if it isn't broke; don't fix it." Technology has no limitations and hackers understand their ability to infiltrate networks or even personal devices are endless.

Every year, Experian, one of the leading data firms, takes a look at what they believe to be the trends to look out for.

Below are five predictions made by Experian and their Data Breach team:

1. Biometric Security

Biometric security has been thought to be one of the most secure ways to keep data safe. Biometric security uses unique characteristics of a person, such as voice pattern, retina pattern of the eye, or fingerprint patterns. It is thought to be extremely difficult to infiltrate. However hackers can steal or alter theses security measures, sensors can be manipulated and spoofed.

2. Cellphones are at just as much risk as computers and laptops. Experian predicts a major attack on cellphone carriers that will simultaneously disrupt usage of both android and iPhone users. Because a majority of the population relies on cell phones to conduct business and personal transactions, such disruption could cause the nation to be at a standstill.

3. Skimming. Skimming is an old tactic, however, it has proven to be a reliable hacking scheme. Skimmers are hidden devices designed to steal card information and passcodes. Hackers will try to expand and not only target ATM machines but also will try to infiltrate complete networks.

4. The cloud. The cloud has always been a phenomenon and used as a tool to store data. Experian believes hackers will set their sights on trying to compromise major cloud companies and, if successful, could have major impacts on sensitive data being exposed.

5. Gamers are not immune. Gaming is big business and hackers know that. Technology has made the online gaming industry explode. Gamers can now connect with others from all over the world. But because of these new advancements, they have become a target. Bad actors will try and pose as legitimate gamers and steal personal and credit card information

Sources:
https://www.techrepublic.com/article/5-major-data-breach-predictions-for-2019/

START 2019 WITH A CLEAN MACHINE

"Making sure you have the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats."

Each year, we want to start out with valuable information that will help our readers. We believe that starting the year with a clean machine and a clean email account is imperative. It's time to get rid of the old and bring in the new!

Many of us have unsolicited emails clogging up our email inboxes. The worst thing to see when you open up your Outlook, Gmail or Yahoo! account is hundreds and hundreds of spam emails. But the even bigger issue is that spam can become a security risk to you and your PC or mobile device. So take the "out with the old and in with new" approach and 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 incoming 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 address.

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. Keep security software current. Making sure you have the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats.

8. 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!

Happy 2019!

Sources:
https://www.stopthinkconnect.org/campaigns/keep-a-clean-machine-campaign