First Bank & Trust Company
Member FDIC

Volume 4, Issue 3

March 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

Is your data safe?

Did you know 90% of the world's data was created only a couple of years ago? That equals to 2.5 quintillion bytes of data per day. That is not a number you say often but it is worth noting that that number will increase rapidly. Data has proven to be a gold mine for bad actors and due to high profile breaches, the highest level of scrutiny has been placed on financial intuitions to ensure their data is safe and that their customers and organizations are protected. But this task has proven to be more difficult to put into action than in theory.

Many banks have implemented the "big data" mentality and have used it to assist with anticipation and planning of real time events. This tactic is great, but the banking infrastructure has always been a complex entity, and as the landscape for technology changes so quickly, it makes it hard to stay one step ahead. So the question is: do you know where your data is and is it safe? That is the challenge not only for banks but for all businesses. Many experts believe data centralization is the name of the game. Although there have been skeptics that disagree and believe that housing all information in one location is literally a Disney World for hackers, it has gained enormous support throughout the IT community. Here is how the experts explain their thinking. They believe that by breaking down the mine of fixed data that an organization does not regularly use in its day-to-day operation and then centralizing the data, it is more likely to increase visibility across an organization, thus allowing it to stay in a real time environment. This has shown to be beneficial when making long and short term business decisions. Centralizing the data also allows an organization to view data coming in and out that can be regulated by device, user, and location. What is equally important as having all data in one location is also having the information encrypted.

Encryption has been an indispensable tool in technology and many are calling for the federal government to step in and make it mandatory to use encryption for all organizations that have any digital information. Some believe that is a bit extreme and heavy handed, but with many recent security attacks on large companies, it seems to now be a necessity. Failure to inadequately encrypt sensitive information can lead not only to hacker's infiltrating the data, but also to regulators publicly bringing down the hammer on those who find themselves in a security breach kerfuffle.

The public is also becoming more tech-savvy and paying close attention to how financial intuitions and other companies handle the data they store.

Continue page 2

And with social media, it makes it very convenient for dissatisfied customers to voice their concerns and demand change with 280 characters or less.

The good news is there are several resources and software programs that fit the need of every budget and size company. And there are new ways to keep the data encrypted while it is in use allowing the information to never be decrypted on the server and remaining in the hands of the owner of the data.

Having complete control of data is crucially important, especially to those in the financial sector who have compliance and regulations they must observe. Most consumers don't understand the logistics or technical terms about storing or encrypting data. What they want to know is that their information is safe. So coming up with the best plan for storing data and ensuring it is secure should always be top of the priority list.

Sources:
https://insidebigdata.com/2017/03/21/big-data-big-challenges-keeping-information-safe/
https://www.huffingtonpost.com/brendan-hannigan/ibm-big-data-secure-big-data_b_2853128.html

Stay Connected Safely

Having a chai latte at Starbucks while you work? At the airport trying to kill time by surfing the Net before your connecting flight? Oh, yes; the beauty of public Wi-Fi! Wi-Fi capability has been one of the best inventions for mankind! No more being stuck in one place to use your devices. Now you can travel the world and ALWAYS be connected. But as with all great inventions, there are risks. It's hard to be without Wi-Fi access, so be sure you are always cautious when accessing unknown Wi-Fi sources .

There is a misconception that using public Wi-Fi is just as safe as using the Wi-Fi at home or work. Not the case. Public Wi-Fi is the place where your laptop, tablet and smart phone are most vulnerable. Not having a password to get connected is hacker heaven! It has been shown countless times that hackers can manipulate the Wi-Fi to make you think you are accessing a legitimate connection when in fact you're connecting to a major TRAP! So here are a few things to keep in mind before you get connected.

When you can, always connect to a VPN- A virtual Private Network routes your traffic through a secured network even on public Wi-Fi. There are some free VPN services that you can research but a paid VPN service gives guarantees you are secure.

Avoid automatically connecting to Wi-Fi hot spots- The beauty of the new smart phones and tablets is you can connect automatically to any available Wi-Fi hotspot, no matter where you are. But one must proceed with caution. Not only does this feature allow you to connect to public networks, it also can connect you to malicious networks just waiting to steal your personal information. It is always best to disable that feature on your tablet or cell phone.

Enable your firewall-Most devices have a built in firewall to monitor connections. It may not be foolproof, but it is a step in right direction in keeping your devices safe.

Turn off your sharing capabilities- In a public setting anyone can gain access to your files, logins and personal information if this feature is not turned off.

Don't access your banking information on your smart phone or tablet using public Wi-Fi networks- Hackers on public Wi-Fi networks can spy on what you are doing, therefore making it extremely easy to make your life difficult if they get ahold of private information. You are better off accessing you banking information at home or using your bank's mobile app if you really need to make a transaction when out and about.

Last, but certainly not least; make sure your antivirus and antispyware are up to date- Ensuring your laptops, smart phones and tablets have the most recent software versions is one more tool to help protect you from malicious activity.

Sources:
https://staysafeonline.org/
https://lifehacker.com/top-10-ways-to-stay-safe-on-public-wi-fi-networks-1791800347