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

Volume 4, Issue 2

February 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

Why Encryption is Important

We get pretty outraged when we hear about data breaches and the possibility that criminals may have gotten access to our personal information. It's an all too common story nowadays and we see that even the big companies and organizations aren't immune. That's why, more than ever, it is so important to encrypt any sensitive information you send out electronically.

Encryption disguises information to make it unreadable to unintended individuals. Many types of organizations have mandatory encryption laws that are enforced by regulators. The medical sector, military, and definitely the financial sector, have specific guidelines that must be followed. The banking and financial industry is held to a very high standard and rightfully so. The amount of sensitive information that is electronically transferred over these networks is enormous. Any time you are dealing with credit card numbers, bank statements and customers' personal information, encryption is mandatory and helps create a secure environment for that type of sensitive information.

Although some may want to encrypt everything, including the kitchen sink, a great rule of thumb to use is, if it contains sensitive information, encrypt it.

Here are some good questions to ask yourself when deciding to encrypt a file:

⇒ ***If the information was on paper instead of in digital form, would you shred it before you threw it out?***

⇒ ***If the information was seen by someone who shouldn't have seen it, could that person do something malicious with the information?***

Any sensitive data that needs to be protected for regulatory compliance, or to comply with internal policies and standards, or confidential business information and intellectual property, should always be encrypted. We have all heard the horror stories about stolen laptops and the devastation that is wreaked when those laptops fall into the hands of a cybercriminal.

Other than the mandatory encryption guidelines, deciding on what data to encrypt is typically based on the risk of disclosure. But all organizations that hold sensitive information should employ strong encryption practices sufficient enough to protect information from being subverted by prying eyes that are up to no good.

Sources:
https://us.norton.com/internetsecurity-privacy-what-is-encryption.html
https://www.trendmicro.com/vinfo/us/security/news/online-privacy/encryption-101-what-it-is-how-it-works

4 Best Practices for Internet Security

We are early into the new year and it is worth revisiting one of the most important steps that we can all take to protect our information.

We all love having access to the Internet. We can stay connected to our family and friends, go shopping, and make travel arrangements; but we also need to pay close attention to protecting ourselves and our personal information. Experts projected two years ago that by 2018, more than half of the world's population will be on the Internet, along with a total of some 21 billion devices. Wow!

"Experts projected two years ago that by 2018, more than half of the world's population will be on the Internet, along with a total of some 21 billion devices."

Having that many people and devices on the Internet leaves the door open to many cyber criminals. If you are not concerned about the likelihood of such attacks, you should be.

Here are some basic security best practices you can employ to protect yourself.

1. *Keep your software up to date - Hackers are constantly looking for vulnerabilities in software to penetrate. This is why it is extremely important to be diligent about applying the patches and updates that your software providers issue.*
2. *Use strong passwords on everything- Using the same password for everything seems like a good idea in theory, but that is exactly what a hacker is banking on. Change your passwords often and make sure to not reuse previous passwords.*
3. *Don't over share- Social media is a great way to keep up with friends and family but sharing too much information over the Internet can be problematic. What many don't realize is that there are some companies that scan social media outlets to collect data on you that can possibly deliver malicious payloads to your devices.*
4. *Don't click on pop ups- Especially the pop ups that say your device has been infected with malware. It's a scam! Clicking on a pop up may download malicious malware on your device that requires you to pay money to have the virus removed.*

These tips are not new and we have heard them all before. However, it is extremely important to make sure these tips are ***implemented***. Take extra precautions while online to avoid scams, viruses and other malicious attacks. The above are some of the best tips that can keep you safe while enjoying the Net!

Sources:
https://business.verizon.com/smallbizresources/internet-security
http://www.zdnet.com/article/10-security-best-practice-guidelines-for-consumers/