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

SEPTEMBER 2019 Issue 9

7 SOCIAL MEDIA SAFETY TIPS

Let's face it, social media is no longer a trend; it is the norm. The millenniums don't know of a day when there were no smart phones, smart TV's or social media.

Social media has literally taken over almost every aspect of our life. There is not a day that goes by when we are not asked to "like, "post or "retweet" something. There has been a significant shift in every industry like education, tech, and even banking to make social media a part of their business strategy.

As technology becomes more and more advanced, so do the social media outlets. Providing more capabilities to stay connected than ever before, social media users want the companies they deal with, including their banks, to be able to connect with them on all levels. Research shows 65% of Americans use one or more social media platforms and that number is set to rise each year.

However, with "likes" and "retweets" come risks--not just for you, but your family, friends, and employer. But there are some key steps to making your social media experience more secure. Below are some tips to help keep you safe while enjoying the social media platforms.

<u>Posting</u>
Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or even the jobs you can get. If you don't want your family or boss to see it, you probably should think twice about posting it.

Continued on page 2

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

Lock Down Your Privacy Settings

Almost all social media sites have strong privacy options. However, most are defaulted to a certain setting. It is your responsibility to make sure your security settings are set appropriately to protect your privacy and your information. So before posting take time to go through all the options available. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

Scams

Just like in email, bad guys will attempt to trick or fool you using social media messages or even ads. Sometimes clicking on those ads can take you to sites where a cybercriminal may try to trick you out of your password or credit card or possibly steal that information if you believe it's a legitimate site to make purchases on.

Think Before You Click

Be careful what you click on: If a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend. Before you click on anything be sure it is from a trusted source.

Terms of Service

Know the site's terms of service. Anything you post or upload might become the property of the site. Basically, read the fine print!

Strong Passwords is a MUST

Secure your social media account with a long, unique password such as a passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

Know Your Work Social Media Policy

Before you post anything about work or from a work device check with your supervisor first to make sure it is okay to publicly share or even use a work computer to access social media sites.

Following these tips can help make social media a much safer online experience. To learn more on how to use social media platforms safely check your social media site's security page.

Sources:
https://carleton.ca/its/2016/social-media-safety/
https://www.experian.com/blogs/ask-experian/9-ways-to-stay-safe-on-social-media/
https://www.sans.org/security-awareness-training/resources/top-tips-securely-using-social-media

THE

WHAT, WHEN AND HOW OF BACKUPS

What are backups? Now more than ever the term "backups" has been at the forefront of many roundtable discussions with IT professionals. As we have seen data breaches reach record numbers as well as natural disasters have become more catastrophic, data has never had to be more protected than now.

Backups are copies of your information stored somewhere other than on your computer or servers. When you lose valuable data, you can recover that data from your backups. Unfortunately, too many people fail to perform regular backups. But before you start backing up your data you first need to decipher what you want to back up. There are two approaches: (1) backing up specific data that is important to you; or (2) backing up everything, including your entire operating system. Every organization must decide based on importance what they should or need backed up.

When should you backup data and how frequently? This is always a question asked. Built-in backup programs, such as Apple's Time Machine or Microsoft Windows Backup and Restore, allow you to create an automatic, "set it and forget it" backup schedule. Common options include hourly, daily, weekly, etc. Other solutions offer "continuous protection," in which new or altered files back up immediately each time you save a document. Again, depending on what type of data it is and where it falls in line of importance can help an organization prioritize when and how often certain data needs to be backed up.

Finally, the how. How you are going to back up your data is also an important decision. There are two common ways to back up your data: physical media or Cloud-based storage. Each approach has advantages and disadvantages. However, deciding on which approach to use will need to be a thoughtful decision which takes into account your business environment and network infrastructure. Physical media is devices you control, such as external USB drives or Wi-Fi accessible network devices. The advantage of using your own physical media is it enables you to back up and recover large amounts of data very quickly. The disadvantage of such an approach is if you become infected with malware, such as ransomware, it is possible for the infection to spread to your backups. Also, if you have a disaster, such as fire or theft, it can result in you losing not only your computer, but the backups as well.

Cloud-based solutions are online services that store your files on the Internet. Typically, you install an application on your computer. The application then automatically backs your files, either on a schedule or as you modify them. An advantage of Cloud solutions is their simplicity–backups are often automatic and you can usually access your files from anywhere. Also, since your data resides in the Cloud, home disasters, such as fire or theft, will not affect your backup. Finally, Cloud backups can help you recover from malware infections, such as ransomware, as many Cloud solutions allow you to recover from pre-infected versions. Some of the disadvantages include the amount of time it takes to back up or recover very large amounts of data. But as technology changes and advances so will the timeframe for this solution. Also, privacy and security is important. Storing your data with a third-party vendor does have risk and should be weighed appropriately when making a decision on this type of service.

Having backups of your data is the one the most important things you can do. In the event of a disaster, theft, computer crash or any other unfortunate mishaps not having your data accessible can be costly to your organization. It is also imperative to test your backup system and process to ensure that data is correct, usable and saved in the appropriate places. Testing will also allow you to see any loopholes that need to be addressed.

Sources:
http://legacy.novabackup.com/importance-of-backing-up-your-data-at-home-and-at-work/
https://www.sans.org/sites/default/files/2017-12/OUCH-201708_en.pdf