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

April 2017 Volume 3 Issue 4

Is Your Data Backed Up?

Our computers and servers house all of our very critical data. Could you imagine losing all of it? For some, that would be the equivalent to the end of the world. Data is the most important asset for companies. Essential emails, financial information, documents, pictures are all at risk of being lost permanently if backups are not regularly done. Data on many devices contain everything and anything that keeps businesses operating smoothly on a daily basis which is why it is crucial to ensure that data is being backed up consistently.

There are several ways that data can be lost: hardware failure, viruses or malware bugs, human error, cyber criminals or natural disasters. No one knows when any of the above can take place and it always happens when you least expect it. If your data is not properly backed up, it can cost a significant amount of time and money to recreate that information. Some organizations are required by law to remain compliant and keep certain information on file for a certain number of years. Backing up your data is a way to protect your company, your customers and your employees in the unfortunate event something does go wrong. Data should be backed up once or twice daily and ideally, organizations should have a backup schedule in place that is regularly performed. As an added measure of protection, you may even use several different procedures of backing up data in the event one system fails.

Having all your data in one place is dangerous. Studies have shown that major data loss has been detrimental for some businesses. 43% of businesses never recover from a major data loss and end up going out of business within one to two years after the event. Just backing up the data is not the only step to alleviate this problem, however. You also have to test your back up process to ensure it works and that the data can be restored. There are plenty of ways to back up data but every organization must find a method that works for them and ensure that that method is verified and tested at least twice a year. Preparing for the unexpected with a solid approach on backing up data will help minimize the risk of organizations losing irreplaceable information.

Sources::
https://msdn.microsoft.com/en-us/library/bb727010.aspx
http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/backup-of-data-files-why-it-is-important.aspx
http://www.atlanticbusinesssystems.com/blog/importance-data-backup-disaster-recovery

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

In this issue:

The Importance of Two Step Verification

Security breaches, from hacks on cell phones to hacks of Fortune 500 companies have increased substantially over the past several years and what experts have evaluated is that most of these are related to passwords. Cracked passwords are valuable to cyber criminals, often offering significant monetary gains. They can be bought and sold on the dark web just like buying and selling stocks on the stock market. High bidders know that cracked passwords provide extraordinary access, inevitably making their hacking jobs a lot easier. With advancing technology, methods of protecting information need to be progressive as well. At a minimum, experts believe that two-step verification should be standard for everyone.

What is 2 Step Verification and How Does it Work?

Two-step verification is also known as two-factor authentication, TFA or 2FA. It is an 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. Although not foolproof, it makes it harder for a cybercriminal to gain access to users' accounts. There are three types of authentication factors that are commonly used:

- ***Knowledge Factor*** such as a PIN (Personal Identification Number) or a Password
- ***Possession Factor*** such as a Security Token or an ID Card
- ***Inherence Factor*** also known as biometrics such as a fingerprint, or voice/eye/face recognition

2FA would require that a user have two out of the three above factors in place. For example, in order for you to access your account at an ATM, you must have a bank card (possession factor) along with a valid PIN (knowledge factor). This method helps confirm the identity of the person accessing the account, thus lowering the amount of identity theft cases and breaches perpetrated through phishing scams or other methods used by hackers to obtain passwords.

Studies have shown that 51% of users reuse the same password over several accounts making them extremely vulnerable to being hacked and 82% of businesses admit that "fake" accounts are a real issue. It has been reported that large organizations have spent over 14 million dollars to try and combat these issues and encourage the use of 2FA. Organizations hope that if a cybercriminal is able to steal a password they will not be able to penetrate a user's account because they are not in possession of one of the other factors. Also, if the account is compromised, with 2FA, many times the user will be alerted with a prompt about an access code. The access code would be something the hacker would need to fully log in to a user account. This will help victims of these types of cybercrimes recognize a potential problem which would prompt them to immediately change their passwords or notify someone of a possible breach.

Although 2FA has been around for some time and is not a new concept, it has recently become a major talking point with IT experts in light of the major hacks that have taken place. Nowadays, you will find mobile devices as well as PCs and laptops and several online accounts offering 2FA. The standard use of user name and password have proven not to offer as much protection as once thought, underscoring the need for 2FA. As 2FA becomes more common the hope is that the number of password hacks will reduce dramatically and prove to be a valuable tool in the fight against password based cybercrimes.

Sources:
https://gcn.com/articles/2015/04/09/2-factor-id.aspx
https://www.rapgroup.net/blog/what-is-two-step-verification-and-why-is-it-so-important/
https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/