FEBBRUARY 2019
ISSUE 2

First Bank & Trust Company

The Bank That Puts You First

Member FDIC

Inside This Issue

EQUAL HOUSING LENDER

Member FDIC

Good Versus Bad

Best Way to Create Safe Passwords

Passwords. They have to be difficult enough to not be easily cracked, yet easy enough for the user to remember. What a dilemma. But passwords is a very necessary part of conducting personal and professional business online. It is the first line of defense that can either help or stop a cybercriminal.

In the right network environment, users get prompted to change their passwords every 30 to 90 days. For many, this can be overwhelming. Many users tend to recycle passwords because, let's face it, it's easy. However, reusing the same password across multiple social media accounts and websites, can be a goldmine for a cybercriminal. All a hacker has to do is a quick cross reference check of password and email combination and, voilà, he's in! Even making slight changes to old passwords is nowhere near foolproof. Keep in mind that there are hackers out there whose only job is to crack passwords.

Last year, studies showed more than 16 million people had their identities stolen. That is up from the previous year. Once a hacker has just one password from a user, he can probably hack into all of the other user's accounts…leaving a trail of mayhem.

Choosing an effective password can be difficult, but here is a list of good versus bad techniques to use when changing passwords.

GOOD

- Think of your favorite song! Using a lyric from one of your favorite songs may be a difficult task for a hacker to break, but easy for you to remember. Example: ***wearetheworld.*** But be careful not to use songs that you have listed as favorites on your social media pages or other outlets.
- Think of a memorable phrase from your all-time favorite movie! Example: ***goaheadmakemyday.*** Again be sure to use a movie that you do not have listed as your favorite on your social media sites or other outlets.

Sources:
https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords
https://www.forbes.com/sites/kateoflahertyuk/2018/12/14/these-are-the-top-20-worst-passwords-of-2018/

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

- Mix it up a bit. Use symbols to replace letters. If your password is "sample" you can replace the ***"s"*** with a dollar sign and the ***"a"*** with the at sign. Example: ***$@mple.***
- Don't skimp on characters. Your password should be at a minimum of 8 to 12 characters and be a mixture of numbers, symbols and capitalizations. Example: ***G@oDp@sS067g!*** These types of passwords tend to be more difficult for users to remember however, they also make it more difficult for a hacker to crack.

BAD

- Never use your date of birth or dates with significant importance (e.g., birthdays, anniversaries, etc.). This type of information could be easy for a hacker to find.
- Don't' use words in the password that pertain to the application being used. For example if you are logging into your bank account the password should not have anything containing the word bank. Example: ***banking25$.***
- ***123456*** is still a very bad password and unfortunately is still being used. It is considered the most popular password that is hacked.

If you feel that your passwords may be unsafe, take the time to update it to a stronger one now, while your accounts are secure. It can possibly save you a lot of regret in the future.

" Think of a memorable phrase from your all-time favorite movie!"

Top Five IoT Vulnerabilities

"Internet of Things" (also known as "IoT") has been around since the late nineties. It is the concept of connecting every day devices and appliances, such as phones, tablets, cars and even coffee machines to the internet. It is a great concept in theory and has yielded some great returns and benefits. Reducing the amount of time it takes to complete a task is one of the great benefits of everything being connected at all times. However, there are some vulnerabilities that should not be taken lightly. Below are the top five vulnerabilities of IoT:

1. Insecure Network Services - Most IoT devices have tools for diagnostics and testing. However these are probably not tested with the rigor that is needed, thus making them susceptible for their code to be exploited. Every time a new feature is added to the IoT device it leaves room for more security holes to be exposed.

2. Lack of Encryption- When data is transmitted from one device to another or through the internet, it is in clear text unless encrypted. Without the encryption anyone can read that data.

3. Privacy Concerns- If there is no encryption, important and sensitive information can be exposed to hackers. Your personal information such as your date of birth, social security number or even personal conversations can be out in the open.

4. Weak or Default Passwords- A password is usually the first line of defense against hacking. If an IoT device uses a default password or if the password is guessable, the end user is at great risk.

5. Patch Concerns- Patches are extremely important in order to close security loopholes and to find flaws before they end up wreaking havoc. It has not been clear if all IoT devices have proper patching protocols in place.

Find out if your new coffee machine that is now connected to the internet can be fixed if a patch is required. If not, you may want to consider disconnecting it from the internet.

The reality is we are connected to the internet more than ever before and that will not change. As a matter of fact, statistics show that by 2020, more than 31 billion devices worldwide will be connected to the internet. With that in mind, it is important to consider security vulnerabilities when purchasing IoT devices and understand all the risks.

Sources:
https://datafloq.com/read/5-Security-Vulnerabilities-Looming-Internet-Things/2127
https://www.beyondtrends.com/article/top-10-iot-vulnerabilities-of-2018/4134/10