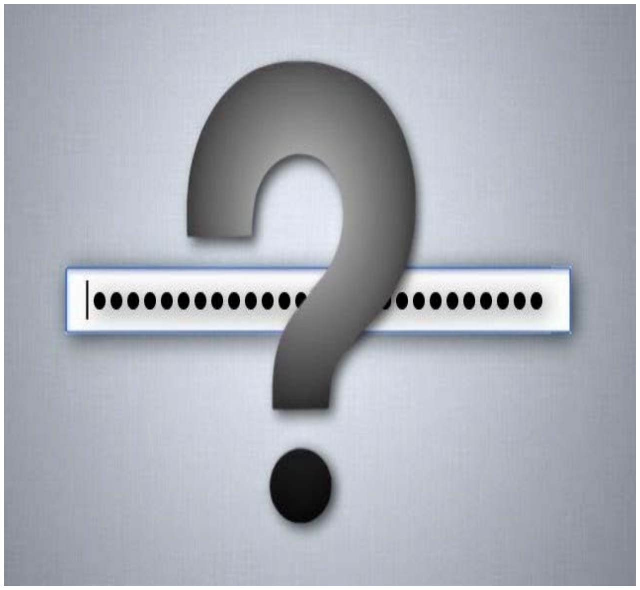
First Bank & Trust Company
The Bank That Puts You First
Member FDIC

March 2017
Volume 3, Issue 3

Password Reuse is a Big No No

Passwords. They have to be tough enough that no one can crack the code, but easy enough that you can remember. Password protection 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 looking to hack your accounts. In 2016, researchers found many social media accounts for sale on the dark web which exposed personal information. The likelihood that your account has been hacked via your password unbeknownst to you is extremely high. And reusing passwords does not help; in fact it is one of the biggest mistakes one can make .



Our passwords are like our favorite, go-to, familiar sweater. But like that favorite sweater that you eventually have to get rid of to replace with one that is better designed to keep you warm, so do you have to replace your password with one that is equally or more robust to keep you safe. When someone reuses the same password across multiple social media accounts and websites, it is literally like finding a pot of gold at the end of the rainbow for a hacker. All a hacker has to do is a quick cross reference check of password and email combination and voilà, they're in!

Creating a different password for every account should be quite simple, but who has the time (and creativity) to create (and remember) different passwords for each and every online account? It sounds like a chore, but today more than ever, it is an essential necessity in online safety. Although many websites are getting better at recognizing the last several passwords used and forcing the user to create something different, cyber criminals are still extremely savvy. Having good password hygiene and not reusing old passwords is more critical than ever before. Password reuse is a huge risk that can possibly lead to data breaches within organizations and personal information leaks of individual users.

Sources:
https://betanews.com/2015/07/30/59-percent-of-consumers-reuse-passwords/
http://www.pcworld.com/article/219303/password_use_very_common_research_shows.html

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

In this issue:

There are a few things that can be done to help protect you, though:

√ Don’t use stale passwords. Change your passwords and user names at least every 30-60 days.

√ Use strong passwords and stay away from date of birth, anniversary dates, etc. Get creative and use symbols and numbers which many sites now make a requirement when creating a password.

√ Use a different password for every single website or account you set up online; that way, if a hacker gains access to one account it will be harder to gain access to other accounts. Yes, it is tedious, but necessary. In the end, you may have 20 different passwords to keep track of but wouldn’t you rather be safe than sorry? If keeping track of so many passwords becomes overwhelming, research different tools to help keep track of passwords in a secure way.

√ Use two factor authentications when possible.

√ This is a given, but worth reiterating: don’t share your passwords.

Security Training-A Never Ending Task

Protecting data and financial information is a top priority and an ongoing task for many organizations. There are plenty of software applications and other tools that can help do this, however having the best technology can only be effective if all employees within an organization know their roles and responsibilities in safeguarding information. Fifty-nine percent of data breaches take place because of unknowingly negligent employees and that percentage makes many security professionals concerned. The number indicates that despite the high amount of breaches over the past several years, security training for employees has still not become a top priority for many organizations.

Unfortunately, employees have unknowingly provided a hacker with pertinent information too many times through schemes like phishing. Phishing has become one of the best and cheapest ways for a hacker to gain access to a company’s information. The phishing game has become more sophisticated and the methods have evolved, making even the most knowledgeable user vulnerable. But because of the lack of security training, more and more cyber criminals are able to breach a company’s network. Organizations need to recognize the limitations of their chosen software applications and security devices and need to understand the importance of the role of their employees.

One of the most important fundamentals of any cybersecurity plan is ensuring there is a clear security policy in place and that every employee adheres to those guidelines set in that policy. In addition, each employee must have mandatory and frequent training. Technology is one of the fastest growing sectors and things change rapidly. Something that was status quo yesterday can be replaced with something new within a week. Policies and practices will change based on the evolution within the industry and employees need to be made aware when these changes take place. The training should not only serve to educate employees of the ever-changing security threats such as malwares, phishing attacks, social engineering attacks and viruses, but it should also serve as a way to engage employees so that they see cybersecurity as something that is a necessary tool to incorporate in their daily duties. The training should provide them with the tools to make good, sound decisions, and when in doubt, to know the proper steps to take. There are some basic key points that employees should be constantly reminded of such as keeping a clean machine, making sure they use strong passwords and that they are changed frequently, to be leery of emails from unrecognizable names and email addresses, and to be mindful of strange activities happening on their computers.

Training employees on an ongoing basis is a crucial part of fighting against cybercrimes and should not be overlooked. Employees need to understand that they, too, play a very important role in keeping the company and its customers’ information safe. Your employees can be the weakest or strongest link and that is all determined by the investment made into training them properly and consistently.

Source
http://www.prnewswire.com/news-releases/employee-errors-cause-most-data-breach-incidents-in-cyber-attacks-300342879.html
https://www.symantec.com/connect/blogs/training-your-employees-information-security-awareness
https://staysafeonline.org/business-safe-online/train-your-employees