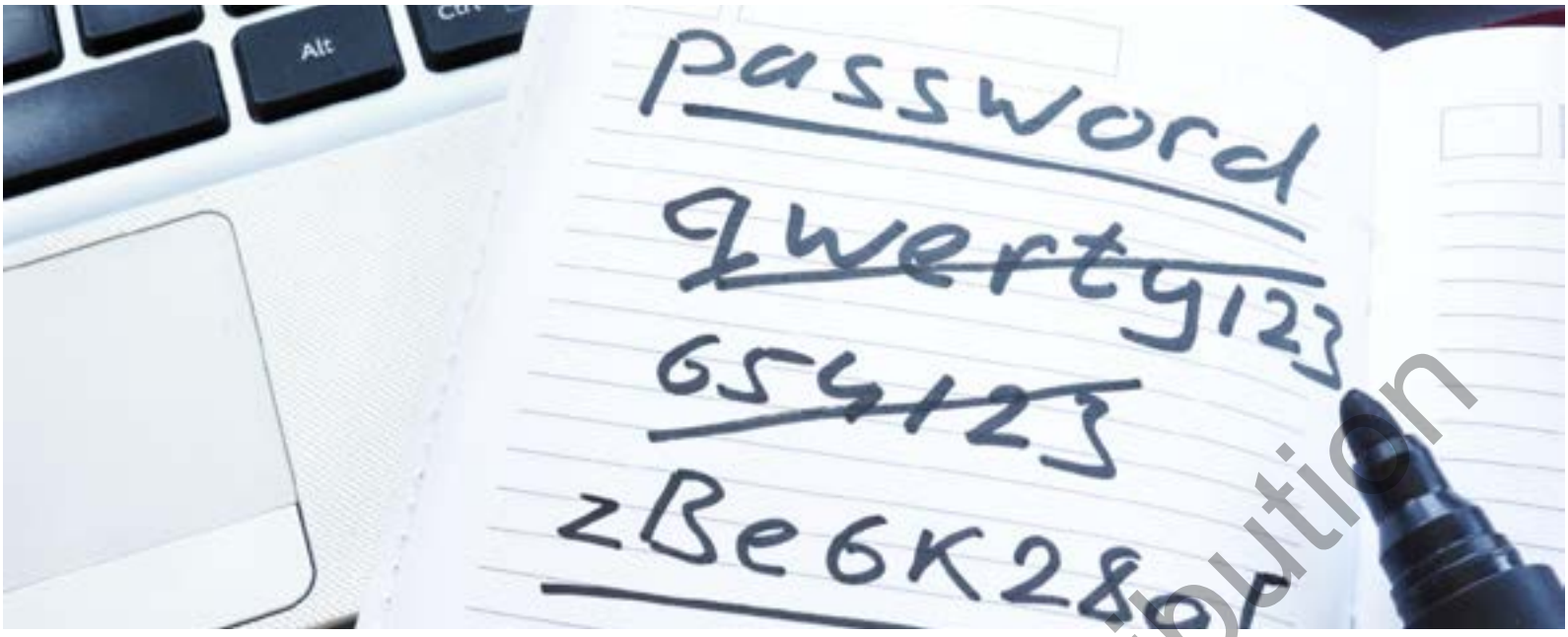

Teresa S. Sampleton, CFP®, CPA
Vice President
Sampleton Wealth Management

230 Park Ave. West
12th Floor
New York, NY 10169

(888) 336-6884

teresa.sampleton@SampletonWealth.com
www.sampletonwealth.com

How to Create Ultra-Secure Passwords That Keep Hackers Away

By Devin Kropp, Horsesmouth Associate Editor

With data breaches occurring more and more, it is important to protect personal information stored in online accounts with secure passwords. The majority of passwords do not pass the test. Learn how to create a password that will keep your data safe online.

Would you rather wash the dishes than create a new password for an online account? If you chose the dirty dishes, you are not alone. According to a study by Harris Interactive and Janrain, 38% of those surveyed would prefer doing household chores over creating a secure username and password combination. And when we finally sit down to create these passwords, we don't seem to be that good at it.

According to Instant Checkmate, 73% of people use the same password for multiple sites. Even scarier, 33% of people use one password for every site they visit.

With weak passwords all over the Internet, researchers at Imperva found that it would take an expert hacker under 20 minutes to break into 1,000 different accounts. That doesn't leave you with very good odds.

The number of identity theft cases is growing every day, and hackers can gain access to your life by breaking one password. A study done by Javelin Stategy found that one person becomes a victim of a hacked account every two seconds—a total of 13.1 million victims in a recent year.

Chances are, once hackers gain access to one of your accounts, they will be able to gain access to many more accounts by trying the same password or resetting your password if they have broken into your email. Take Wired writer Mat Honan: Once a hacker got into his Apple ID account, his Twitter, iPhone, Mac, and Gmail accounts were all compromised. The hacker went so far as to clear Honan's hard drive clean, deleting pictures of his child's first year, which are now gone forever.

But there are steps you can take to make your passwords secure and keep the hackers out.

PASSWORD DON'TS

- **Avoid common passwords.** Researchers at Instant Checkmate found that the most common password of 2012 was "password." That doesn't make a hacker's job very hard. Protect yourself by avoiding passwords that are commonly used and first for hacker's to guess, such as "12345" or "abc123."
- **Avoid passwords that can easily be guessed.** Next on a hacker's list of possible passwords? Your name, your spouse's name, you child's name, your pet's name, your birthdate, etc. Any information you share on social media acts as clues to your password for hackers. For that reason, it is important to stay away from details that could be found easily through your online presence. Even if you do not use social media, you should not use these details as passwords. Hackers may be able to gain access to this information through other means.
- **Avoid dictionary words.** While there are millions of dictionary words to choose from, a simple lowercase word is not a secure password. Hackers know which words are used most often—and if your password is one of these words, it won't be long before they break in.
- **Don't use the same password for multiple accounts.** By using the same password over and over again, you are making a hacker's job easy. Once they gain access to one of your accounts, they will likely try that same password to get into other accounts you have. If the password is the same, they can easily wreak havoc on many different aspects of your life.

Now you know what not to do. So how do you create a secure password? Let's say right now your password is "finance." Let's go through the steps to take that weak password and transform it into a safe and secure password you can use.

PASSWORD DO'S

- **Passwords should be at least eight characters long.** Longer passwords are generally more difficult to hack. Instant Checkmate found that the average password is only six characters long—not enough characters to keep hackers out. Our example of "finance" is only seven characters long and at the moment is a weak password.
- **Use letters, numbers, and symbols.** Using all three types of characters makes it more difficult for hackers, as there are more variables they have to get right. So instead of "finance," your password could be: finance/8$. While that is better, we can still improve this password's strength.
- **Use both uppercase and lowercase.** Again, this adds security, as there are more details a hacker would have to guess. With this new rule, "finance/8$" could become: FiNance/8$. Better, but we can still do more.
- **Use a mnemonic phrase.** As we discussed earlier, dictionary words are easier to hack. But passwords containing dictionary words are easier for us to remember. There is a way to create a password that is strong—and easy to remember. If you can remember a sentence, you can remember a secure password. Think of your favorite song, poem,

prayer, or pledge. Take a line from that and use the first letter of each word to construct your password. For example, take the Beatles' "Strawberry Fields Forever." The first line, "Let me take you down, 'cause I'm going to Strawberry Fields" is memorable and can be transformed into a secure password you can use. Taking the first letter of each word of that line your password becomes "LmtydcIgtSF." Now, of course, we need to add some numbers and symbols. Your final password could look something like this: Lmtyd_cIgtSF/76. If you are a Beatles fan, this password will be easy to remember but hard for the hackers to break into.

- **Use a goal-setting password.** Rather than have your password be a mental drain, use it as a step to achieving your goals. Think of something you want to accomplish in the next year and use that as your password. For example, say your goal is to get in shape and lose 10 pounds. Take the first letter of each of those words and add some numbers and characters: Gis&L10lbs!. Now you have a password that is motivating and strong.
- **Use two-factor authentication.** Many sites now offer two-factor authentication when logging into accounts. For example, when logging into a site with two-factor authentication enabled, a code will be sent to your phone that you must enter after your password to gain full access. In order to log in, you must have your password and a special code that is changed every time. If a hacker successfully guesses your password but does not have your phone, they cannot get into your account. Currently, sites such as Gmail, Facebook, Dropbox, Twitter, and more offer this service. Many banks and credit card companies offer this service for online use as well.

It is important that you apply these rules to all of your passwords and create new, unique passwords for all of your different logins. It is also suggested that you change your passwords at least twice a year.

PASSWORD SERVICES

If the thought of creating multiple secure passwords and remembering them all seems daunting, there are services that can help.

1Password is software you can download that will store your login credentials for each site. After downloading the program, you will be prompted each time you log in to a site to save that password into your 1Password account. Your 1Password account is protected by a master password (the only one you have to remember). In order to access any of your other passwords saved in the software, you must enter your master password to retrieve it.

This program can also generate strong passwords for you, and since you don't have to remember them yourself, they can be long and almost impossible to remember—making them extremely difficult to hack. All your passwords are encrypted, meaning that even 1Password doesn't know what they are. If you forget your master password, you lose access to your password list. 1Password does not offer two-factor authentication at the moment, but your registered device is needed to access your password list, which does add more security. The program is available for Macs, PCs, smartphones, and tablets.

Dashlane also uses one master password to store all of your logins. Once you sign up, Dashlane will begin to save your logins for each site that you browse. The next time you visit that site, Dashlane will automatically log in for you. This service can also help you generate strong passwords. Your passwords are encrypted and then decrypted locally, so they are known only by you.

The service also has a multifactor authentication option that adds an extra level of security to your passwords. You can download the basic service for free, or you can get the premium service, which gives you unlimited access to Dashlane on all your devices, including desktop, laptop, smartphone, and tablet. Dashlane is compatible with iOS and Android.

KeePass also protects all of your logins with one master password. The service also protects you from keyloggers. A keylogger is malware that a hacker can install on your devices that keeps track of everything you type, making it easier to hack your accounts. KeePass protects against this through its Auto-Type feature, which automatically pastes your password into the password box of a site. There is an additional plug-in you can install within KeePass to set up two-factor authentication to add more security. KeePass is available for PCs and Macs as well as smartphones

and tablets. Best of all, this service is completely free to download and use.

UPDATE TODAY

An easy way to protect yourself from thieves looking to steal your identity is by creating strong, secure passwords for all of your accounts. Following these tips can help you transform an easily hackable password into a secure password, better protecting your identity and personal information stored online. Don't let the hackers in—update your passwords today to stay safe.

Devin Kropp is an associate editor at Horsesmouth. She is the co-author of the award winning book, Hack-Proof Your Life Now! and is a co-creator of Horsesmouth's Savvy Cybersecurity program.