A Special Report from Hughes Financial Services, LLC

SAVVY CYBERSECURITY

WAYS TO IMPROVE YOUR SECURITY & KEEP YOUR IDENTITY SAFE

IN THIS REPORT

HUGHES FINANCIAL SERVICES, LLC

2201 Cooperative Way ▪ Suite 150 ▪ Herndon, VA 20171
(703) 669-3660 ▪ F (703) 880-4905 ▪ www.h4fs.com

How to Create Ultra-Secure Passwords That Keep Hackers Away

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 Strategy found that one person becomes a victim of a hacked account every two seconds – a total of 13.1 million victims in 2013.

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 in 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 hackers to guess (such as "12345" or "abc123").

Avoid passwords that can be easily guessed

Next on a hacker's list of possible passwords? Your name, your spouse's name, your child's name, your pet's name, your birth date, 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 the hacker's job easier. 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 a 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 "LmtydcIgoSF." Now of course, we need to add some numbers and symbols. Your final password could look something like this: Lmtyd_cIgoSF/76. If you are a Beatles fan, this password will be easy to remember but hard for the hackers to break into.

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 into 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 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. 1Password for a desktop costs $49.99; it's $14.99 for an iPhone/iPad. The app is free for Android phones and tablets.

LastPass also uses one master password to store all of your logins. Once you sign up, LastPass will begin to save your logins for each site that you browse. The next time you visit that site, LastPass 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 for $1/month, which gives you unlimited access to LastPass on all of your devices, including desktop, laptop, smartphone, and tablet. LastPass is compatible with iOS, Android, Windows Phone, and Blackberry.

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.

Child ID Theft: 8 Steps to Keep Your Kids Safe

You are not the only one who needs to be on guard about their personal data safety. Minor children are 35 times more likely than adults to suffer ID theft. Here's what parents (and grandparents) need know.

The latest target of identity thieves is not you, but rather your children. With little to no financial history, minors make an unsuspecting and easily exploited target. According to the 2012 Child Identity Fraud Survey, conducted by Javelin Strategy and Research, one in 40 households has had one child who has suffered from identity theft. In fact, children are affected by identity theft and fraud 35 times more frequently than adults.

What makes a nine-year-old's identity so attractive? Because children are not financially active, this theft is likely to go unnoticed for years. The majority of parents and guardians do not request copies of their child's credit report, so they don't notice any fraudulent activity. Yet the damage done can affect a child well into his or her adult life.

The theft that keeps on giving

Take Gabriel Jiminez, who shared his story with the New York Times. His identity was stolen when he was a child. His mother discovered the breach in 1993 when she went to file taxes for the work he did as a child model at age 11. The IRS notified her that taxes had already been filed under Gabriel's Social Security number.

That's where Jiminez's frustrations began. His Social Security number had been stolen by an illegal immigrant and used for many years. As an adult, he had issues with his credit reports as well as setting up bank accounts and getting approved for car insurance. Jiminez was denied credit when he tried to set up phone, gas, and electricity in his first apartment because the thief had already created accounts. His credit rating was badly damaged. Jiminez and his mother were able to identify the thief years ago, but that did not release Jiminez from having to prove his own identity time and time again.

He is not alone in this experience. It is estimated that 500,000 children are affected by identity theft each year. Children who have their identities stolen can spend the rest of their lives dealing with complications regarding their personal information and identity. However, there are measures you can take now to try to prevent these never-ending frustrations.

How to keep the thieves away

Protecting a child's identity from thieves and fraudsters is similar to protecting your own identity. The first step is to educate yourself and your children on keeping their information safe. You should also:

Keep all of your children's personal documents locked up. This includes their birth certificates and Social Security numbers, as well as any other documents that contain sensitive personal information.

Protect your children's Social Security numbers. Before you give it out, ask why someone needs it, how they will keep it safe,

and how they will dispose of it. You should also inquire if there is another personal identifier they can use instead. Some schools have started to issue randomly selected ID numbers rather than Social Security numbers to identify students.

Check with your children's school. Some schools share information about their students with third parties. You have the right to opt out of having a child's information shared in directories or online.

Create a joint bank account. When setting up a child's bank account, make sure it's a joint account. This ensures that no one can access the account without your approval.

Opt out of marketing materials. When creating bank accounts for your children, you should also opt out of receiving marketing materials in their name. Children should not be receiving credit offers. A pre-approved credit card offer addressed to your child is a goldmine for identity thieves; opting out ensures that kids will not be sent these offers. If your child starts to receive pre-approved credit cards in the mail, it could be a sign of identity theft. Take proper measures to check your child's credit report and call the company that sent the materials immediately to remove your child's name. You should also add your child's name to the Do Not Mail list. You can do so through the Direct Marketing Association.

Monitor your child's internet usage. Until your children are at an age where they understand the dangers of the Internet, you should monitor what they are doing online. If your child has an email address to communicate with family members or teachers, maintain access to his or her password and check up on who is contacting the child, keeping an eye out for spammers and fraudsters. Set up parental controls and read privacy policies before signing your child up for any online account.

Teach your children how to be safe online. While monitoring your child's accounts online is important, children themselves should also be taught how to keep their information safe on the Internet. Explain to them that they should not share any personal information on the computer (or tablets and smartphones) or visit sites without permission. Advise them to show you any emails before they open them and teach them the dangers of phishing. Explain that by opening emails from people they do not know, they risk accidently giving their personal information to the bad guys. Teach them how to create strong passwords for their accounts and warn them to not use any information in usernames that could be used to identify them (i.e., "JohnDoe").

Update your child's electronic devices. Keep any computer or tablet your child uses up-to-date with antivirus, firewall and other types of security software.

Stay alert. Being aware is the first step in protecting your child's identity. If someone has fraudulently used your child's identity, there will be an associated credit report on file, so it is a good idea to periodically check for a credit report in your child's name. To do so, you should contact all three of the nationwide credit reporting agencies (Experian, Equifax, and TransUnion) and ask them to do a manual search of your child's Social Security number. When doing so, you will need to provide proof that you are the child's legal parent or guardian. You can do so by sending a cover letter with your child's information as well as copies of your child's birth certificate listing you as the parent (or other legal documents for proof of guardianship), your driver's license, and proof of address.

If your child's identity has been compromised, there are steps to take to regain control. First, you should alert the three credit reporting agencies of the fraud. You must request a credit freeze on your child's account so no new accounts can be opened by the thief. You should also file a report with the Federal Trade Commission (FTC) as well as your local police department.

Your own identity is not the only one you have to protect. Following these eight steps can help keep a child's identity away from thieves and fraudsters, and avoid what could become life-long credit issues.

5 Ways to Boost Your Security Against ID & Credit Card Theft

A week hardly passes without news of credit card and identity theft. Here are some security measures you can take, including some you've not likely heard of before now.

About a year ago, I was sitting down to dinner with my family when I got a phone call from a department store inquiring about my new credit card and recent purchases. I knew right away I had a problem because I'd never shopped at that store.

I left my dinner and started my own investigation. I spent dozens of hours tracking the frauds and thefts. I soon learned that five different credit cards had been opened in my name; new debit cards had been issued from my bank; and money had been transferred from my savings and checking accounts.

Naturally, I was completely appalled. Now I'm on a mission to make sure people learn from my experiences and consider putting into place new security measures, many of which I'd never known about – and I'm in the financial services business.

Here are five ways you can improve your protection against fraud:

Create secret "verbal passwords" on your bank and credit card accounts

Verbal passwords on all your bank and credit card accounts will save you time, money, sanity and future chaos. Everyone enters a numbers-based key-code password when withdrawing money from a bank account at the ATM. Some, though not all, retail stores request an ID when you make a credit card purchase at the register. So why don't banks require a password when you make a transaction at the teller?

Most banks won't tell you to request a verbal password or phrase to be placed on your bank accounts. This is the most important thing you can do to protect yourself from the fraudsters lurking out there. Here's how to do it:

Walk into your local bank and ask to speak with the branch manager. When you meet with the branch manager, request to meet in a private office to discuss your accounts. Once in a closed office, instruct the branch manager to place a "verbal passcode" on all over-the-counter and phone request withdrawals, newly issued bank cards, and even transfers.

If the verbal password or phrase is not given, no information or transactions may proceed. I had this type of protection on one of my personal bank accounts. Unfortunately, I didn't do this on the other one that was scammed for thousands of dollars in cash with a teller at a bank in a completely different state.

Most bankers don't even check the signature card when given an over-the-counter withdrawal request. The verbal passcode or phrase will be your guardian and savior. One last thing: when you are asked to give your verbal passcode, never say it out loud at the bank. Ask the teller for a piece of paper, write the passcode down and pass it to the teller. THEN, take back the paper, tear it up, and put it in the trash.

Shield yourself from the "magic wand" with an RFID-protected wallet

While shopping in crowds at the mall can be fun, you can also unknowingly expose yourself to a fraud device known as a "magic wand."

"Wanding" is the process by which all of your credit card information can be stolen by a $20 device that is able to read, record and save it all in an instant. This information is then illegally used to create multiple cards that will be sold without your knowledge and permission.

You can stop this scam from happening by shielding your credit cards with an RFID-protected wallet (Radio Frequency Identification Device). These wallets can cost from $30-$200. They have a built-in shield that deflects any credit card reading/skimming devices. Another cheap, quick, and useful fix is to wrap your credit cards in foil. Yes, tin foil. This may sound crazy but it works. I happen to like a product called the Flipside Wallet (www.flipsidewallet.com).

Protect your credit file like a pro

If you really want to control your credit file, open an account at one of the three credit bureaus: Equifax, Experian, or TransUnion. This is the best way to examine the accuracies of your credit history and manage your credit future. This service costs approximately $17.95/month.

Opening an account gives you the power to lock or unlock your credit file. It's your virtual credit file switch. Once you lock your credit file, no one can open a new credit card account – not even you. If you want to open a new credit card account or receive a bank loan, you have to log into your account and unlock your file with one flick of a virtual switch. This service also notifies you via email or text when key changes occur to your credit profile and if there is suspicious activity on any of your important financial accounts.

Never let your credit card leave your sight

When you're shopping or eating at a restaurant, think twice before your hand over your credit card for payment. When your card leaves your hands and is out of your field of vision, this is when it can have its information stolen via a smartphone camera or mini card reader called a skimmer. This type of fraud can happen in the moments you are waiting to get your card back. The best defense is to be present when your card is swiped (funny word, huh?).

Avoid making in-store credit card applications

I love to save money, especially during the special promotions and the holidays. Most stores will offer immediate credit and an attractive discount on all new purchases with a new on-the-spot application and approval.

Who is handling your paper application once it has been given to the store clerk? This information can be exposed to many unsavory people. If you really want the credit card and a special discount, you can call the company's credit department or fill out an application online ahead of time.

This protects you in several ways. The information you have given is with the headquarters representative. The conversation is usually recorded and stored. Once your application is approved and processed, it's mailed to your home address. This will help keep your information safer.

You may have to call a company representative for any in-store or online promotions that may be used with your newly minted cards.

Protect yourself with these security measures

Any time of the year is a good time to turn over a new leaf and better protect your credit card and bank accounts. Through my experience, I believe that these safety measures will save you some precious time and unnecessary headaches.

How to Create Ultra Secure Passwords that Keep Hackers Away, Child ID Theft: 8 Steps to Keep Your Kids Safe – Devin Krupp is a New York-based writer for Horsesmouth, LLC.

5 ways to Boost Your Security Against ID & Credit Card Theft -- Bryan Mills is a New York City writer.