PASSWORDS & DUAL-FACTOR AUTHENTICATION

PASSWORDS

By now, you are probably well aware of the need to password protect your accounts and devices. Most now require password protection, though it wasn't always that way. However, despite the constant admonition to use a "strong" password and to follow certain guidelines, many people still fail to do so.

HIGH-RISK ACCOUNTS

When we refer to **login credentials** we mean your user name and password. Online **accounts** require login credentials. Devices usually require credentials but they might be optional. It seems like everyone wants you to create an account, so it's helpful to think in terms of **high-risk accounts** and **low-risk accounts**. High-risk accounts are the kind which, if accessed by a bad guy, could easily lead to having your money or identity stolen. They include:

- Banking and financial accounts
- Healthcare accounts
- Work or school accounts
- Email accounts
- Social media accounts
- Shopping accounts

Email and social media accounts can also be used by scammers who want to impersonate you in order to scam others.

Low-risk accounts are everything else – news or sports websites, for example.

HOW PASSWORDS ARE STOLEN

Understanding how bad guys obtain passwords will explain why basic password hygiene is so important.

PEOPLE LEAVE THEIR PASSWORDS LYING AROUND

The most obvious is the classic “password written on a sticky and attached to the computer” – people actually do this. However, if you record all of your passwords in a text file on your computer or in the cloud, you are also asking to have your passwords stolen.

PEOPLE USE EASILY GUESSED PASSWORDS.

A list of the most commonly used passwords can be found here. Using any of these is the equivalent of having no password.

If you are being specifically targeted, scammers can research you and focus on things like pet names, partner and child names, dates of birth, sports teams, etc. to guess your password.

Also, replacing the letter “O” with the number “0” or the letter “I” with the number “1,” or appending a number to the end of a common password, doesn’t make it more secure.

25 Most Common Passwords (2018):

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. 696969
18. shadow
19. master
20. 666666
21. qwertyuiop
22. 123321
23. mustang
24. 1234567890
25. michael

PEOPLE ARE TRICKED OUT OF THEIR PASSWORDS

Have you ever received an email or gotten a call from “tech support” or “your bank” asking for information about you? Scammers are very good at convincing people to tell them their passwords. Jimmy Kimmel has a famous bit where he shows how easy it is to get strangers on the street to reveal their passwords.

Similarly, **phishing** is a scam where you receive an email from someone pretending to be a person or business you know in order to either get you to click a link or attachment that will download **malware** (“malicious software”), or to trick you into logging onto a fake website, thereby giving away your login credentials.

VIRUSES AND MALWARE

Bad actors use various means to load malware onto computers that might search for any stored passwords or intercept your password when you enter it into a login screen. **Keyloggers** record all of your keystrokes, and can either be malware or a physical device attached to the computer.

HACKERS STEAL PASSWORDS THROUGH DATA BREACHES

One of the prime targets of a data breach is login credentials. Hackers know that many people use the same password in multiple places, so they will steal credentials from one business, and then try to use the same credentials at banking and other websites until they find one where the user happens to have an account. Some hackers steal credentials and resell them to other hackers on the **dark web**.

What a hash looks like:

Password: 123456

MD5 Hash:
e10adc3949ba59abbe56e057f20f883e

SHA3 Hash:
64d09d9930c8ecf79e513167a588cb75439b762ce8
f9b22ea59765f32aa74ca19d2f1e97dc922a3d49545
94a05062917fb24d1f8e72f2ed02a58ed7534f94d27

Changing 1 character creates a totally different hash

Password: 123457

MD5 Hash:
f1887d3f9e6ee7a32fe5e76f4ab80d63

SHA3 Hash:
a78de06400cbfd377c66bded0a2f9ee95cc8e3fefb4
8060038e75753a304430147bd59f4ba157bbfb0d95
9c0412f9c41cb46e242f2a87a2b509013a2c758bc53

When a hacker steals credentials, what she is actually stealing is **hashes** of the credentials. A hash is a one-way encryption technique that converts your password into gobbledygook that *cannot* be decrypted. This is why, if you lose your password, the business will offer to reset your password, but cannot tell you what your password is. They don't know! They only have the hash – whenever you login in, the same hash algorithm (process) is run on your password, and the two hashes are compared. In that case, you might wonder what can a hacker do with a bunch of unreadable hashes? Because there are a limited number of hash algorithms (like SHA-3 and MD5), the hackers just create every password they can think of, and then hash them all and put them into a **hash dictionary**. That way all they have to do is look up the hash and cross-reference the actual password. Hash dictionaries may have millions of entries. This is why common passwords are such a bad idea – they definitely exist in the hash dictionaries.

The Have I Been Pwnd website will tell you if your credentials have been stolen.

HACKERS “BRUTE FORCE” THE PASSWORD

A **brute force attack** is where the hacker just tries every possible combination of password until he gets it right. This is why many websites lock your account after a certain number of tries and why longer passwords are better – every additional character makes the time to do a brute force attack increase exponentially.

One way to know how long it will take to crack a password is to try it in the How Secure is My Password website. **Note:** Don’t use your *actual* password in this site.

PASSWORD BASICS

• NEVER SHARE YOUR PASSWORD

This seems obvious but that means with *anyone* including someone who calls or emails you pretending to be tech support and asking for your password. This is a common scam. No legitimate business or professional will *ever* contact you and ask you for your password.

Also, you might be tempted to share your password with a friend or loved one – that’s a risk you might take, but ask yourself, “Is this person as capable of protecting my password as I am?” Your password is only as safe as the least safety-conscious person who knows it.

• NEVER WRITE DOWN YOUR PASSWORD

Also don’t keep a “**plain text**” (unencrypted) file of your passwords. If you don’t want to forget your passwords, use a **password manager**.

• USE A PASSWORD MANAGER

A password manager is an app or other software product that stores all your passwords securely. It can usually also generate new strong passwords and autofill password fields. Password managers **encrypt** your stored password information and require a **master password** to unlock them (that’s a password you definitely don’t want to forget and *definitely* don’t want to write down).

Some password managers are standalone apps, others are built into your browser or your operating system (like Apple’s keychain). The browser/OS managers might give you the option to enter your master password whenever you want to use it to autofill a password. Requiring the master password every time might be a pain, but you definitely want to make sure you have a master password, and make sure it is required sometimes.

Password managers also sometimes can store other sensitive, non-credential information like bank account and credit card numbers.

• BE CAREFUL WITH AUTOFILL

Having your browser, OS, or password manager automatically fill in your username and password is incredibly convenient. You should never autofill certain passwords, however – mainly, financial and banking websites, but consider declining autofill on other high-risk accounts. Remember that your security is only as strong as its weakest link. Financial accounts generally automatically log you out after a short time, but even with this feature, if you leave your laptop where someone else can get to it, and your browser auto-fills your bank login information, that means anyone who gets on your laptop will be able to access (and empty) your bank account.

When you fill in a password, your browser may ask if you want to save it. For these kinds of websites, select "never ask me this."

• USE "STRONG" PASSWORDS

We will address this below.

• USE UNIQUE PASSWORDS

If you use a different password for every website, then even if hackers breach one website, the others will be safe. Password Managers can help generate unique passwords.

• ROTATE YOUR PASSWORDS

This means you should change your passwords periodically. Some companies or websites force you to do this whether you want to or not. You should change your passwords at least once per year (some say 6 months). This way, even if someone manages to steal your password, it will no longer be useful to them once you have changed it.

• TRACK YOUR PASSWORDED ACCOUNTS

You should know all of the accounts that have asked you for login credentials. This way when it comes time to change your passwords, you know which websites to visit. This can be difficult given that every website wants you to make an account these days. Even if you cannot remember *every* site where you have an account, you should at least be mindful of your high-risk accounts.

If you store all your accounts on a password manager, then tracking is easy.

• NEVER ENTER YOUR PASSWORDS ONTO PUBLIC COMPUTERS

Public computers often have malware on them like keyloggers specifically to harvest passwords. A common scam is for bad guys to put a physical keylogger onto library computers during tax season in order to collect data from people filing taxes.

• NEVER ENTER YOUR PASSWORDS ONTO WEBSITES THAT DON'T HAVE HTTPS

Every **URL** (web address) starts with **HTTP**:// or **HTTPS**://. HTTPS means that your information is encrypted from when it leaves your computer to when it arrives at the destination. HTTPS is now used almost everywhere, particularly on high-risk websites. No web designer should *ever* create a login page that doesn't use HTTPS. If you see a website still using HTTP, that means not only is your information not safe and easily intercepted, but the designer of that site clearly knows nothing about security generally and you should avoid using it.

Some web browsers no longer show the start of URL's, but they will show a lock or other message to inform you whether the website is secure or not.

• NEVER ENTER YOUR PASSWORDS ON PUBLIC WI-FI

Hackers are able to intercept Wi-Fi signals on public Wi-Fi (like at the airport or a coffee shop). Some even set up their own fake Wi-Fi networks in order to collect your data directly. If you have a smart phone and need to log into a banking site, turn off Wi-Fi and use the cellular network instead.

STRONG PASSWORDS

The common wisdom seems to be that a "strong" password is at least 8 characters long, not a common word, and is made up of numbers, special characters, and upper and lower case letters. Some say the password should be at least 10 characters, but the longer, the better.

From what we've learned so far:

- A **long** password is harder to brute force
- A **unique** password is safe even if your other credentials are stolen
- An **uncommon** password is less likely to be in a hash dictionary
- A password that doesn't rely on information about you is harder to guess or scam

Password managers or **password generator** websites can create completely random, strong passwords. There is only one problem with them: they are not **memorable**. That's not a problem if you are sure you'll always have your password manager at hand, but if you want a strong *and* memorable password, I recommend a method that has worked for me.

THE STRONG AND MEMORABLE PASSWORD GENERATION FORMULA

STEP 1: Think of a memorable phrase and take its acronym

"Can't Buy Me Love" = cbml

STEP 2: Add a special character (because most websites require one)

cbml?

STEP 3: Look at the name of the website and drop the last character (or the first, whichever you want – some websites won't let you use the full website name in your password)

cbml?amazo

Step 4: Capitalize one of the letters, according to a formula you know (like second letter of the website)

cbml?aMazo

Step 5: Add on a number of some length (the three digits of your phone number after the area code? Your parents' zip code?)

cbml?aMazo25609

And you're done! Believe it or not, this is a very easy password to remember. The first few times you use it you'll run through the steps, but quickly it will become second nature to type it. And each password will be unique to a website:

cbml?fAcebo025609

cbml?gOogl25609

This is a password that is unguessable, not in any hash dictionary, long, and unique.

DUAL-FACTOR AUTHENTICATION

Sadly, no matter how good your password is, there is always a risk that your account can be compromised. You might have your password stolen by a clever phishing attack. A hacker might convince a customer service rep to reset your password and direct the reset email to the hacker.

The readings contain a well-known case where a Wired reporter had his credentials stolen by hackers who tricked Apple's customer service representatives, resulting in the reporter's laptop and phone being wiped clean (all those photos gone!), email account deleted, and twitter account taken over, where terrible messages were sent out under the writer's name. **Dual-Factor Authentication** (**DFA**) would have stopped this.

Some websites have begun to require it, but it is still optional for many. All of your high-risk websites should have dual-factor authentication turned on.

WHAT IS DUAL-FACTOR AUTHENTICATION

Dual-Factor Authentication (sometimes called Two-Factor or Multi-Factor Authentication) refers to account security where you cannot get in without **two** of the following:

- Something you **know**
- Something you **have**
- Something you **are**

Your username and password are two things you *know*, which means that if someone else knows those two things, they can access your accounts. Username and password are *not* Dual-Factor Authentication.

An ATM Card and PIN are something you *have* (the card) and something you *know* (the PIN), so it is Dual-Factor. If your card is stolen, the thief can't use it without the PIN. If someone learns your PIN, it's useless without the card.

Something you *are* refers to biometrics, which is a method of authentication using unique information about our bodies like a fingerprint, retinal scan, or facial recognition. Requiring both a password (*know*) and a thumbprint (*are*) would be Dual-Factor Authentication.

Websites have implemented Dual-Factor Authentication a few different ways. The most common is to ask for your mobile phone number, and when you want to log in a code (usually 6 digits) is texted to you. You are then asked to type in the code. This way, you must log in using your credentials (something you *know*), but anyone without your mobile phone (something you *have*) won't be able to get the code. Some websites give you the option of emailing you the code or calling you with it.

Some websites allow you to designate your computer a "trusted" computer, which means that it doesn't ask you for the second factor every time you log in from that computer. In a way, you are designating that computer or device as something you *have*, so it becomes the second factor. If a hacker with your credentials can get access that computer they could still access your accounts, but they cannot if they're sitting halfway around the world.

AUTHENTICATOR APPS

While the Dual-Factor Authentication method above is vastly better than not using it at all, there is an even more secure way to implement DFA. This is because clever hackers have actually figured out how to replicate your mobile phone by tricking your phone company into providing them with your SIM card (the tiny chip that identifies your phone). If a hacker manages to change your phone number for your account, they can also intercept the second factor.

Thus, a *more* secure technique is to install an **Authenticator App**. The most popular Authenticator Apps right now are Google Authenticator and Authy. Some password managers like 1Password and LastPass also have Authenticator Apps built in.

To use an Authenticator App, you install the app on your phone and, when you turn on DFA on a website, the website will show a QR Code (that square weird-looking bar code). You use your phone's camera to read the code, and the App sets up a new authenticator for that website. The authenticator then generates a new 6-digit code every 30 seconds.

Now, rather than the website texting you the code, you just open up your authenticator app and type the 6-digit code it shows into the website Because the authenticator is synced with the website for your account, the website accepts the 6-digit code.

Now, the *only* way a bad guy can get into your account, even if he steals your credentials, is with your specific Authenticator App on your phone synced to your account.

AUTHENTICATOR DONGLES

The latest in DFA is **authenticator dongles** (also called **keys** or **tokens**). This is basically a small USB device that you plug into your computer to authenticate yourself. The dongle is something you *have*.