Password Security

by Mike KA9CQL
ka9cql@gmail.com
2021-10-14 v4.7

* Passwords are Just Electronic Locks
	+ Give you a sense of security
	+ Prevent “nosey neighbors” from snooping around
	+ Help businesses ensure it’s “really you”
	+ They help keep “bad guys” out
* The Problem with Passwords…
	+ Too many – they’re needed *EVERYWHERE*!
		- Which password goes with which account?
	+ Good passwords are hard to remember
		- Complicated website password requirements
			* “Use capital and lower case letters, numbers, special characters… at least three of these, no more than two of these from any one group in a row, no common words, blah blah blah” – OMG, seriously!?!?
	+ Oh, and don’t forget to change your password every few months, every time there is a breach or “suspected breach” – “out of an *abundance of caution*”…. (If they were using “an abundance of caution” in the first place, there wouldn’t be a breach – am I right?!)
	+ Every website has a “forgot-your-password?” link
		- “Set it, then forget it!”
* How Humans Adapt
	+ (Because they’re needed everywhere) We tend to reuse the same one!
		- Problem: If just one website gets hacked, there goes all your security!
	+ (Because they’re hard to remember) We tend to use “mental shortcuts”
		- Popular “shortcuts” -
			* Birthdays
				+ “04051990”
			* Street address
				+ “1640Cumberline”
			* Phone numbers
				+ “9518675309”
			* Spouse/Child/Grandchild/Pet’s name(s)
				+ “jessica”, “michael”, “walter”, “husband”
				+ “jessica”, “daniel”, “jordan”, “princess”, “sunshine”
				+ “kitty”, “buster”, “snoopy”, “grover”
			* Common words/phrases/quotes
				+ “password”, “monkey”, “changeme”, “qwerty”, “123456”, “chocolate”
				+ “secret”, “god”, “admin”, “root”, “superuser”, “master”
				+ “letmein”, “iloveyou”, “f..kyou”, “bettersafethansorry”, “fourscoreandsevenyearsago”
			* Favorite, famous, popular or well-known movies/characters/actors/historical figures/band/brand/city/sports team
				+ “wargames”, “starwars”, “MatrixRevolutions”
				+ “spongebob”, “captainkirk”, “wonderwoman”
				+ “FranklinDRoosevelt”, “Marconi”, “jesus”
				+ “nirvana”, “barbie”, “yamaha", “samsung", “hotmail”, “nascar”
				+ “losangeles”, “chicago", “boston”
				+ “DaBears”, “angels”, “dodgers”, “yankees”
			* Numbers-in-place-of-vowels
				+ “p4ssw0rd”
			* Numbers/special characters at the end
				+ “password123”
			* …and various combinations
				+ “Spring2021”, “Summer2021!”,etc.
				+ “Jenny8675309”
				+ “admin123”
				+ “Mexico1984#”
	+ (Because websites have reset-password links) We just hit the link!
		- Reset-link is sent via email or text message (SMS)
		- Problem: Email isn’t secure
			* Anyone that wants to can read it as it passes along
				+ China (LOL) …but, seriously – China!

China has no shame in continually re-routing Americans’ Internet traffic “by accident” (read: on purpose)

India does this sometimes

Google “BGP Hijacking” – it’s a DAILY occurrence!

* + - * + Your Internet provider
				+ Your “free” email provider (Google – I’M LOOKING AT YOU!)
				+ Any company/country/service-provider between the email sender and you!
				+ H4ck3rs (\*hackers)

A myriad of Internet-based attacks

(Don’t get me started!)

Classic “Man-in-the-Middle” attacks

Phishing / “Click-bait”

DNS Poisoning

Recommendation: Use OpenDNS

Recommendation: Use Secure DNS

(In your browser)

Paid “insider”

(Can’t do too much about this…)

Public Wi-Fi

Recommendation: Use a VPN!

Hackers – if they have your computer/phone/browser already….

* + - * Did you **reuse** that same website password on your email account!??!?!
		- Problem: Two-Factor Authentication (2FA) isn’t totally/always secure
			* Overwhelming majority of 2FA utilizes email, text messaging or a call to your cellphone as the “second factor” (“first factor” is your password, which you forgot!)
			* By now, criminals already know, or have easy access to, almost everyone’s email address and cellphone number. Some of their information sources -
				+ Telemarketing and traditional/direct-marketing companies
				+ Lexus Nexus searches
				+ Social Media companies
				+ Facebook – tracks you even if you don’t have a Facebook account
				+ Google – tracks *everybody* on the Internet
				+ Your Internet Service Provider (ISP) – They make $$ by selling your data!
				+ Your cellphone company – sells your data – including location!

Don’t need GPS - they triangulate/multilaterate your location, continually!

Triangulation uses angle-of-arrival (non-5G cell towers can’t generally deduce this; this is a required capability for 5G towers)

Multilateration uses time-of-arrival (all cell towers can do this; 5G towers do this exceptionally well)

* + - * + Website tracking companies – hundreds of well-known companies
				+ Credit reporting agencies – they collect/sell your email and cellphone info!
				+ “Underground” / “hacking” websites and data-traders
				+ Data breaches – EVERY MONTH another data breach is announced, and user records get stolen…
			* Hackers can attack/overcome 2FA, too! (More on this in a minute)
* Hackers Adapt, Too!
	+ Bad guys know we take “mental shortcuts”!
		- They use every known combination of these shortcuts to build lists of passwords to try
		- They steal passwords from websites, and figure out the most common patterns
		- They use machine learning to try to predict these, and other “shortcuts”
		- They can download password lists from the Internet
			* <https://github.com/danielmiessler/SecLists/tree/master/Passwords>
			* <https://weakpass.com/wordlist>
			* <https://wiki.skullsecurity.org/index.php/Passwords>
			* <https://gist.github.com/roycewilliams/226886fd01572964e1431ac8afc999ce>
			* [https://en.wikipedia.org/wiki/Wikipedia:10,000\_most\_common\_passwords](https://en.wikipedia.org/wiki/Wikipedia%3A10%2C000_most_common_passwords)
	+ Your account might get hacked *directly*
		- Many hacking techniques can be used against your accounts
			* Brute-forcing (keep guessing passwords until one gets them in)
			* Password spraying (try the most popular passwords against every account)
			* Correctly answer your “Security Questions” (uses your social media posts!)
			* Compromise the website, steal the password database, crack it offline!
			* Lock you out on purpose, to make you use your cellphone (text or phone call), which they intercept (see next item!)
	+ Your phone might get hacked *first*
		- “SIM Swapping” Attack – takes over your cellphone’s account!
			* Simple to do – some US carriers are working on making this harder
			* Gives hackers the ability to briefly intercept your cellphone calls and text messages
				+ …which are two of the three most popular Two-Factor Authentication mechanisms!
	+ **You** might get hacked (using so-called “social engineering” tricks)
		- “Social Engineering” – Scammers call or email you, pretending to be your bank/etc.
		- Over the phone - They talk you into revealing information that lets them get into your account.
			* They may even trigger a text-message or email *from your real account/website*, and then ask you to read it back to them “for verification purposes”/”to prove you are who you say you are” (etc.)
				+ *THIS IS A “LIVE” ATTACK*!
		- Within an email – They get you to click on a link that goes to their fake website, which looks exactly like the real website – and get you to enter your password (etc.)
* Dirty-little-secrets about Passwords
	+ Easy-to-remember usually means easy-to-crack!!
		- Estimated time-to-crack a simple, 11-character password
			* <https://password.kaspersky.com/> - “instantly” (CORRECT!)
			* <https://www.generateit.net/password-strength-tester/> - less than 1 second (CORRECT!)
			* <https://bitwarden.com/password-strength/> - 7 hours (Wrong – false sense of security!)
			* <https://www.passwordmonster.com/> - 31 hours (Really wrong)
			* <https://random-ize.com/how-long-to-hack-pass/> - 7,527,508 years and 7 months (Really, totally and COMPLETELY wrong!)
	+ Hackers have “shortcuts”, too!
		- Well-known password shortcuts (covered, above)
		- Password lists
			* <https://github.com/danielmiessler/SecLists/tree/master/Passwords>
			* <https://weakpass.com/wordlist>
			* … and others from earlier…
		- Cracking just one “unsalts” the rest!
			* Highly technical, but if you hear “salt”/”salted” with regard to passwords, understand that this can be reversed/defeated
		- Amazon Web Service (AWS) can be used to crack passwords, too!
		- Graphics cards (GPUs) aren’t just for cryptocurrency mining…
			* They work as password crackers, too!
			* <https://medium.com/hackernoon/20-hours-18-and-11-million-passwords-cracked-c4513f61fdb1>
	+ If “Passwords are Just Electronic Locks “, then computers are “Electronic Locksmiths”
		- Hiring a (physical) locksmith is easy (even 24/7/365!)
		- Hiring a “password locksmith” is easy, too
			* Most-popular-password lists are online
				+ “Plain-text”
				+ “Hashed”
				+ “Most-popular -per- website”
			* Submit to a website and wait a few seconds…
				+ “Rainbow Tables”
			* Be-your-own “locksmith”
				+ “john the ripper”, “Hashcat” – free password-cracking tools
				+ Kali Linux, Security Onion, Pentoo – Linux operating systems pre-configured for hacking/cracking websites and passwords
			* Cracking-as-a-Service
				+ Free – Internet-based: “submit-and-wait”
				+ Paid – Legitimate tools and websites

Very few; be very careful!

* + - * + Paid – “Underground” services (far more dangerous!)

(I wouldn’t if I were you…)

* OK, SO, WHAT SHOULD WE DO!?!
	+ See if your password was already stolen/cracked. If so, change it!!!
		- Check your passwords on Troy Hunt’s website (“Have I been pwned?”)
			* 613,584,246 *real world passwords* (as of this writing, and always growing!)
			* <https://haveibeenpwned.com/Passwords>
	+ Don’t use a “popular” password
		- <https://nordpass.com/most-common-passwords-list/>
		- [https://en.wikipedia.org/wiki/Wikipedia:10,000\_most\_common\_passwords](https://en.wikipedia.org/wiki/Wikipedia%3A10%2C000_most_common_passwords)
		- Check online password lists mentioned earlier
	+ Don’t use a “bad” password
		- “Short is bad”
		- “Simple is bad” (\*But there’s hope, in a minute…)
		- Using predictable/common “shortcuts” is bad
		- Can you help me?
* Here’s Hope!
	+ Making “good” passwords
		- Longer is *not always* better!
			* Longer-but-common (bad)
			* Longer-but-uncommon (better)
		- Password-helpers
			* <https://lastpass.com/howsecure.php> - Simple, clear advice
			* <https://www.generateit.net/password-strength-tester/> - Has “traditional” advice (plus an estimate of time-to-crack)
			* <https://www.uic.edu/apps/strong-password/> - To really “geek out!”
			* <http://www.passwordmeter.com/> - Another “total geek-out” site
		- The “Menifee Mensch” Way!
			* Long-but-“simple” (avoiding shortcuts!)
				+ “Since1960-MyFavoriteTeam?Dodgers!”
				+ “I-married-Janet-on-June-14th”
				+ “Who’sMyWifeOf30+Years?Francine!”
				+ “IAm6Foot3And180#WithBlueEyes”
				+ “Katie\_Tom\_Bruce\_Carol\_And\_11\_Grandkids!”
				+ “I+h8+rutabaga+September+1972”
				+ “Mac1-n2-Cheese3-is4-da5-bomb6!”
				+ “1L0v3H4mR4d10$ka9cql”
				+ “MyDog=Spot;Aol.com@2021”
			* All of these are long, easy/easier to remember, and very complex (read: HARD FOR COMPUTERS TO CRACK!)
			* That last password “MyDog…” has a website in it – change that for each website, and it’ll be obvious what password goes with which account/website!
		- Online password-generators
			* Use reputable sites… don’t “just google it”
				+ <https://www.lastpass.com/features/password-generator> - Strong, reputable
				+ <https://nordpass.com/password-generator/> - Strong, reputable
				+ <https://www.expressvpn.com/password-generator> - Complex, but secure
				+ <https://my.norton.com/extspa/passwordmanager?path=pwd-gen> - A little too complex, for me…
				+ <https://1password.com/password-generator/> - Also “a bit much”
			* Steve Gibson’s password-generator
				+ For the “criminally-insane”/ultra-paranoid among us!
				+ <https://www.grc.com/passwords.htm>
	+ Protecting Your Passwords
		- Use a “password keeper”
			* 1Password - <https://1password.com/>
			* LastPass - <https://www.lastpass.com/> - Caution: They have had issues… (see: <https://en.wikipedia.org/wiki/LastPass#Security_issues>)
		- What about a hardware device/dongle?
			* YubiKey - <https://www.yubico.com/why-yubico/how-the-yubikey-works/>
			* RSA Key fob (some banks offer these – Wells Fargo, for sure!) - <https://www.rsa.com/en-us/store>
			* A word about using your Facebook/Google login…
				+ Same problem as using a single password everywhere -

If hackers crack that one password, *there goes all your security*!

* + What about Two-Factor Authentication?
		- You usually have to turn it on (it’s not on by default… yet)
		- Most “larger”/”mainstream”/popular websites have it
		- It’s good….ish… I suppose… until it isn’t…
		- Just make sure YOU TRIGGERED it, and not a hacker!
			* Don’t EVER tell someone who called you what is in a Two-Factor Authentication email or text message !!
				+ Only tell someone that you called, and even then, only if you dialed a number that you already knew or obtained from a “trusted source” (e.g. bank/credit card statement, bill/receipt, company website, etc.) *NEVER TRUST AN EMAILED LINK*!!!!
* Parting Advice
	+ Change your passwords as you go –
		- Hit that “forgot my password” link!
		- Use good/stronger/”Menifee Mensch” passwords everywhere
		- Never (EVER!) reuse a password!
		- Write them all down if you have to – lock the list in a drawer/file cabinet/safe deposit box
			* Stronger-but-written-down is better than easily-crackable by some hacker in Brazil!!
	+ KEEP YOUR NEW PASSWORDS SECRET!
		- Don’t give them to anyone!
			* Nobody over the phone
			* Nobody over the Internet
			* Never type it into an email/email reply
			* Never click any link found within an email – even if you think that email is legitimate!
				+ Instead, open a “private” web browser tab and type in the well-known website address yourself, *by hand*!
				+ I hate to say it, but this even goes for “forgot my password” emails!

Just take the time, and do this right.

* + - * NO bank, NO website and NO technical support will ***EVER*** ask you for your password over the phone, or in an email. **P-E-R-I-O-D**.
			* All verbal/emailed/etc. requests for your password are from HACKERS!
				+ If you didn’t type in a website address yourself, treat it like it’s part of a (possibly elaborate) scam!
			* Hackers are even better “salesmen” than that car dealer down the street! (And you surely wouldn’t give them your password!)
				+ Remember – with almost *5 BILLION* people on the Internet, surely *at least one of them is a hacker that is* *more clever than you imagine*!!
	+ Buy a new Wi-Fi router (KEEP the old one, too – more on that in a second…)
		- Plan to spend between $79 and $129 for a “good-ish” one
		- Pick a well-known vendor (aka ***no*** Buffalo, Walmart/Staples “private label” brand, etc.)
		- CHANGE ITS DEFAULT ADMIN PASSWORD!!! (OMG, seriously!?!?)
		- Make your new device’s Wi-Fi password STRONG!
			* Make it truly random, long, and write it down
				+ Internet-based robbers aren’t going to invade your home looking for your password log! (LOL)
				+ Cleaning lady better be trusted, anyway!
				+ If it’s a cleaning crew, however…

Put it in a locked drawer, file cabinet, etc.

* + - Place new device *AFTER* your current one
			* Internet provider modem/device –> then your old Wi-Fi device –> then your NEW Wi-Fi device = GOOD SECURITY!
		- Stop using current router for anything except “IoT Devices” –
			* Smart Thermostats, Ring Doorbells, Alexa/Google devices, security alarms
		- Give your guests this “old” Wi-Fi password
		- Don’t have to get too hung up about how strong the old device’s password is…
			* You shouldn’t trust these IoT devices, anyway!
			* …but change it, if you can (sometimes this pain is too great – that’s ok, and understandable)
	+ And, finally, “Just because you’re paranoid, it doesn’t mean they’re *NOT* after you!”

’73 – Mike, KA9CQL