



# MVARC

## P4ssw0rd Security

\*(password)

Presented by Mike Sipin KA9CQL

October 14, 2021



<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>Tr0ub4dor&amp;3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO INCREASE THE ENTROPY BY CHOOSING ONE OF A FEW COMMON WORDS)</p>	<p>~28 BITS OF ENTROPY</p> <p>2<sup>28</sup> = 3 DAYS AT 1000 GUESSES/SEC</p> <p>(RANDOMLY ATTACK ON A NEW PASSWORD WILL TAKE YOU LONGER TO GUESS THAN IT TO REMEMBER IT)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROUBADOR? NO. TROUBADOR, AND ONE OF THE O's WAS A ZERO? AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>2<sup>44</sup> = 550 YEARS AT 1000 GUESSES/SEC</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE. CORRECT?</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



# Agenda\*

\*BTW - Feel free to ask questions at any point

- Introduction – Who am I?
- What are Passwords?
- The Problem with Passwords...
- How Humans Adapt
- Hackers Adapt, Too!
- Dirty-little-secrets about Passwords
- What Should We Do?!
  - Making good passwords
  - One interesting idea...
  - Online Password Generators
  - Protecting your passwords
- Some “Parting Advice”
- Any Final Questions?

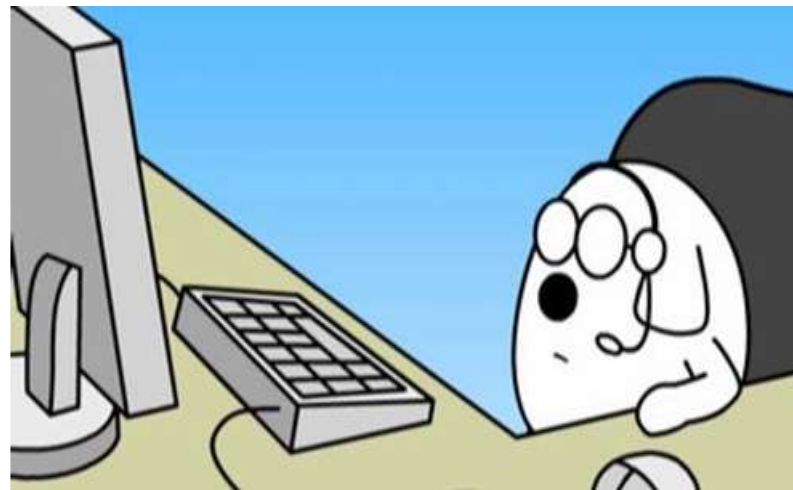


# Who am I?

**Mike Sipin, KA9CQL - Victorville, CA**

**ka9cql@gmail.com**

- Long time Ham
- Professional “hacker”
- Inventor of network-security products and solutions
- Invited to give this talk by Pat, N6WHZ  
(Thank you, Pat!)
- ***Happy to be invited back!***





# What are passwords?



# Passwords Are...

- Passwords are just “electronic locks”
- They give you a sense of security
- Prevent “nosey neighbors” from snooping around
- Help businesses prove it’s “really you”
- Help keep “bad guys” out of your stuff!







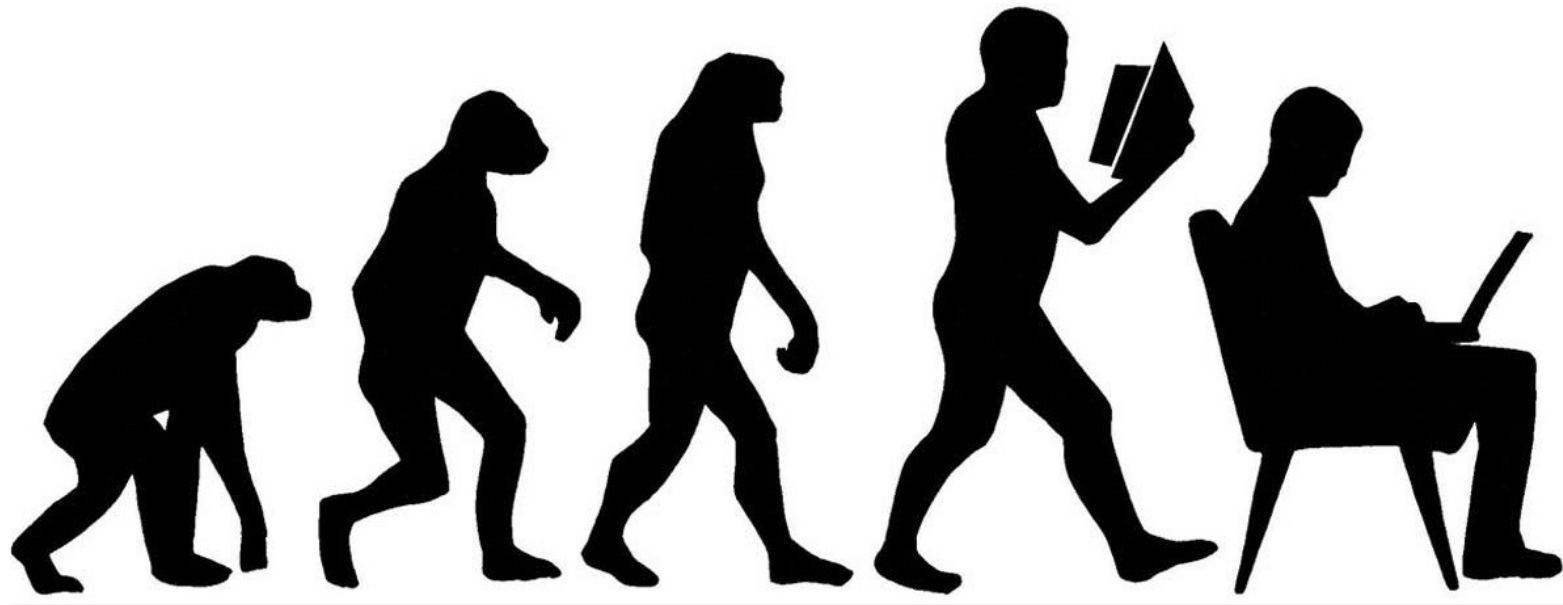
# The Problem with Passwords...



# The Problem With Passwords...

- We need too many! They're used 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 groups, no more than two in a row from any one group, blah blah blah - OMG, SERIOUSLY!?"
- Just when you get a "good one", you are forced to change it!
  - Every few months (company policy)
  - Every time there is a data breach (or even "suspected breach" – they rarely admit it!)
    - Make you change it "out of an abundance of caution". (If they used an "abundance of caution" in the first place, there wouldn't be a breach, am I right?)
- We forget them so often, every website has a "Forgot your password?" link!
  - ...so, we "set it and forget it™!"





# How Humans Adapt

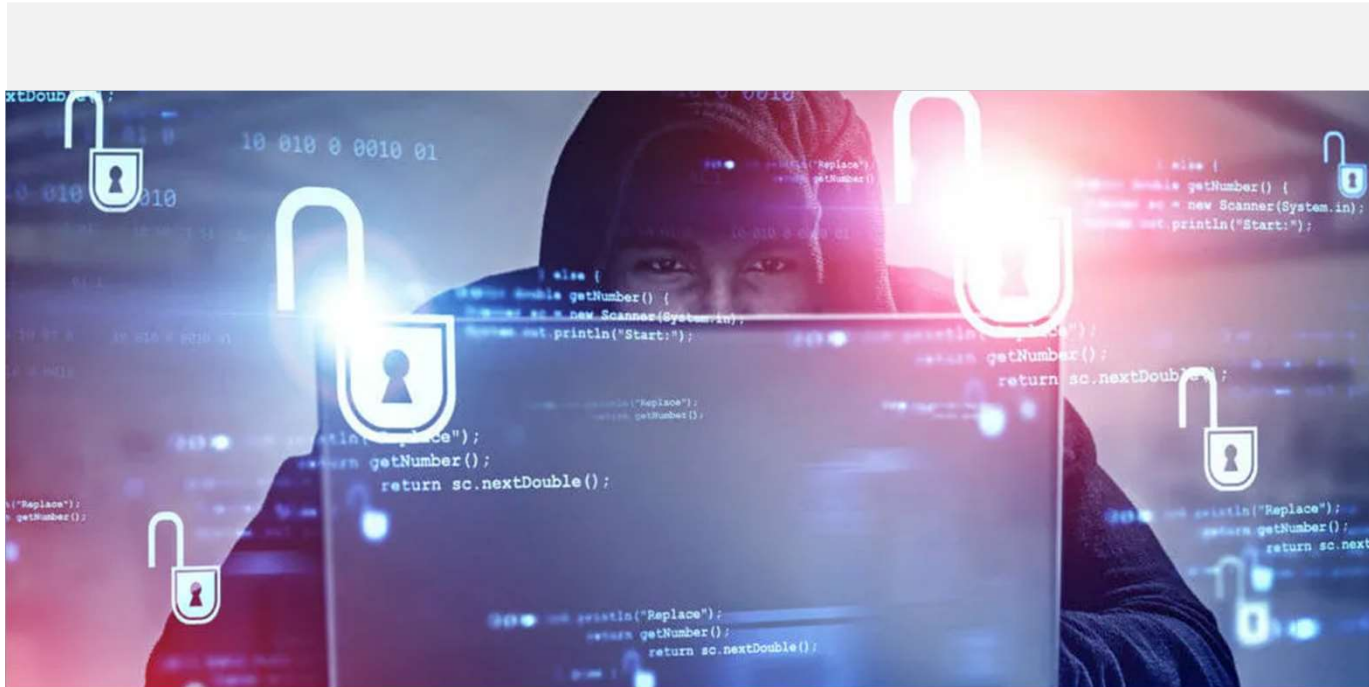




# How Humans Adapt

- (Because passwords are needed everywhere) We tend to *reuse the same one!*
  - Problem: If just one of those websites gets hacked, there goes all your security!
- (Because they're hard to remember) We tend to use “mental shortcuts”
  - Popular “shortcuts” –
    - Birthdays, street addresses, telephone numbers
    - Spouse/child/grandchild/pet's names
    - Common words, phrases, quotes – “password”, “monkey”, “changeme”, “qwerty”, etc.
    - Favorite people, movies, brand names, cities, sports teams (“DaBears” is actually popular!)
    - Use numbers to replace vowels (e.g. “password” becomes “p4ssw0rd”)
    - Add a few numbers to the end of a common word – “password123”, “admin1234”
    - And combinations of the above
      - “Spring2021”, “Summer2021!”, “Jenny8675309”
      - “Mexico1984”, “1l0v3y0u!”





# Hackers Adapt, Too!



# Hackers Adapt, Too!

- Bad guys know we take “mental shortcuts”!
  - They use every known combination of these shortcuts to build password lists
  - Use machine learning to predict human behaviors, and develop new patterns
- Hackers steal passwords from websites
  - Use them directly, as part of “password spray” attacks
  - Use them to try and figure out common patterns to add to their cracking tools
- Download password lists from the Internet
  - <https://github.com/danielmiessler/SecLists/tree/master/Passwords>
  - <https://weakpass.com/wordlist>
  - <https://gist.github.com/roycewilliams/226886fd01572964e1431ac8afc999ce>
  - ...and many more...
- All of these techniques are used to try to figure out your passwords!





# Dirty-little-secrets about Passwords



# Dirty-little-secrets about Passwords

- Easy-to-remember usually means easy-to-crack! (We'll fix this in a bit...)
- Estimated time to crack a simple, 11-character mixed letters/numbers 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!)**
- If these websites say it's easy to crack your password, BELIEVE IT!
- Check each of the above websites, and use the quickest time-to-crack you get – it's likely correct!



# Dirty-little-secrets about Passwords

- Easy-to-remember usually means easy-to-crack! (We'll fix this in a bit...)
- Estimated time to crack a simple, 11-character mixed letters/numbers password –
  - <https://password.kaspersky.com/> - Instantly **(CORRECT!)**
  - <https://www.generateit.net/password-strength-tester/> - less than 1 second **(CORRECT!)**
  - <https://it-easy.com/password-strength-tester/> - less than 1 second (of security!)
  - <https://www.passwordmeter.com/> - less than 1 second
  - <https://www.passwordstrength.org/> - less than 1 second (Really, totally and COMPLETELY wrong.)
- If these websites say it's easy to crack your password, BELIEVE IT!
- Check each of the above websites, and use the quickest time-to-crack you get – it's likely correct!

**Live DEMO**





# Dirty-little-secrets about Passwords

- Easy-to-remember usually means easy-to-crack! (We'll fix this in a bit...)
  - Estimated time to crack a simple, 11-character mixed letters/numbers 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!)**
  - If these websites say it's easy to crack your password, BELIEVE IT!
  - Check each of the above websites, and use the quickest time-to-crack you get – it's likely correct!
- Hacker Tricks
  - They know our “password shortcuts” (covered earlier)
  - They know about password lists, too
    - <https://github.com/danielmiessler/SecLists/tree/master/Passwords>
    - <https://weakpass.com/wordlist>
    - ...and others, from earlier...
  - They use both to try to figure out your passwords!



# More “dirty-little-secrets”...

- If “passwords are just electronic locks”, computers are “electronic locksmiths”
  - Hackers can hire a “password locksmith”
    - Can use online services –
      - Free – Internet based: “submit-and-wait” (usually less than 5 minutes)
      - Paid – Legitimate tools and websites (very few; be very careful!)
      - Paid – “Underground” services (far more dangerous – and far more likely to succeed!)
  - Anyone can become a “password locksmith” (aka “hacker”)
    - “john the ripper”, “Hashcat” – free password-cracking tools
    - Kali Linux, Security Onion, Pentoo – bootable Linux images pre-configured with website and password hacking/cracking tools
    - Amazon Web Services (AWS) can be used to crack passwords, too!
    - Graphics cards (GPUs) work great as password crackers, too!
      - <https://medium.com/hackernoon/20-hours-18-and-11-million-passwords-cracked-c4513f61fdb1>
  - In short, it’s easy to take advantage of anyone that uses a “bad” password!



WHAT  
SHOULD  
I DO



What Should You Do?

# What Should You Do?

- See if your password was already stolen/cracked. If so, change it!!
  - Check your password on Troy Hunt's website ("Have I been pwned?")
    - <https://haveibeenpwned.com/Passwords>
    - 613,584,246 real world passwords (as of this writing, and always growing!)
- Don't use a "popular"/"well-known" or already-compromised 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:10,000_most_common_passwords)
    - Check online password lists mentioned earlier – if you find yours in there, DON'T USE IT!
- Don't use a "bad" password
  - "Short is bad"
  - "Simple is bad" (\*But there's hope coming in a minute...)
  - Using predictable/common "shortcuts" is bad
  - "Can you help me?" – **ABSOLUTELY!**



# 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



# Making Good Passwords

- Longer is *not always* better!
  - Longer-but-common (bad)
  - Longer-but-uncommon (better)
- Password-helpers
  - <https://la...>
  - <https://w...> "l" 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

**Live DEMO**





# Passwords the “Meniffee Mensch” Way!

- Long-but-”simple” (avoiding shortcuts!)
  - “Since1960-MyFavoriteTeam?Dodgers!”
  - “I-married-Janet-on-June-14th”
  - “Who’sMyWifeOf30+Years?Francine!”
  - “IAm6Foot3And180#VWithBlueEyes”
  - “Katie\_Tom\_Bruce\_Carol\_And\_11\_Grandkids!”
  - “I+h8+rutabaga+September+1972”
  - “MacI-n2-Cheese3-is4-da5-bomb6!”
  - “IL0v3H4mR4d10\$ka9cql”
  - “MyDog=Spot;Aol.com@2021”\*
- All of the above 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

- There are websites that will create strong passwords for you!
  - Might not be easy-to-remember them, but they will be very secure!
  - 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

- Write them down, and lock them away (this was mentioned before)
- 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](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/>
  - Google “Titan Security Key” - <https://cloud.google.com/titan-security-key>
  - 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 on other sites...
    - Same problem as using a single password everywhere –
      - If hackers crack that one password, there goes all your security!





# Parting Advice

# Parting Advice (1<sup>st</sup> of 4)

- Change your passwords as you go
  - Hit that “forgot my password” link
  - Use good/stronger/”Meniffee Mensch” passwords everywhere
  - Never (EVER!) reuse a password!
  - Write them all down, if you have to, and lock that list in a drawer, file cabinet, safe deposit box (etc.)
    - 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 address yourself
      - I hate to say it, but this even goes for “forgot my password” emails



# Parting Advice (2<sup>nd</sup> of 4)

- Keep your new passwords secret, continued...
  - Don't give them to anyone, continued...
    - 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
    - Remember – with almost 5 BILLION people on the Internet, surely *at least one* of them is a hacker that *more clever than you imagine*!





# Parting Advice (3<sup>rd</sup> of 4)

- Buy a new Wi-Fi router (KEEP the old one, too – you’ll see why in a second)
  - Plan to spend between \$79 and \$129 for a good-ish one
  - Pick a well-known vendor (no “Buffalo” or Walmart/Staples/Best Buy “private label” brand!)
  - 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 hackers 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 – lock it in a drawer, file cabinet, safe, etc.
- Place new device after your current one
  - Internet provider modem → then your old Wi-Fi device → then your new Wi-Fi device = GOOD SECURITY!



# Parting Advice (4<sup>th</sup> of 4)

- Buy a new Wi-Fi router, continued...
  - Stop using current (“old”) router for anything except “IoT devices” –
    - Smart thermostats, Ring doorbells, Alexa/Google devices, security alarms, etc.
  - 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 (if pain is too great, it’s ok, and understandable)
- And finally.... “Just because you’re paranoid, it doesn’t mean they’re not after you!”





*Any Final Questions?*

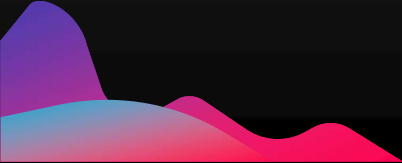



# Thank you, MVARC!

Mike Sipin, KA9CQL



[ka9cql@gmail.com](mailto:ka9cql@gmail.com)



Backup  
Slides  
Follow...

# How Humans Adapt (2<sup>nd</sup> of 3)

- (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, other governments (China, India and hackers routinely, “accidentally” redirect Internet traffic...)
        - Google “BGP hijacking incidents” – Thousands of hijacks per year!
      - Your ISP and free email provider can read it (Google – I’m looking at you!)
      - Any company/service/service-provider between the sender and you can read it, too!
      - ...of course, that includes hackers
        - So many ways to attack the Internet....
          - Man-in-the-middle, phishing, click-bait, DNS poisoning
          - Paid/malicious company insider
          - Public Wi-Fi is “suspect” (“sus”, for you young whipper-snappers!)
            - Recommendation: Use a VPN!
- DID YOU REUSE THAT WEBSITE PASSWORD ON YOUR EMAIL ACCOUNT!?!?!?!?!?





# How Humans Adapt (3<sup>rd</sup> of 3)

- Problem: Two-Factor Authentication (2FA) isn't totally/always secure
  - Overwhelming majority of 2FA utilizes email, text messaging or a phone call to your cellphone
    - These are the “second factor” – (“first factor” is your password, which, you forgot!)
    - By now, criminals already know (virtually) everyone's email address and cellphone number
      - Way too many sources of this information, including hacks/data breaches, Internet tracking/marketing companies, 3<sup>rd</sup> party information aggregators and even *credit reporting agencies!* (Yep, you read that correctly!)
      - Google freely admits that they read all your emails (they say it is “to provide you products and services”... yeah, right!) – and they sell data about you to others
      - Your cellphone company sells your information – including your location information!
      - And, of course, social media companies are notorious for how much of your information they collect and sell to 3<sup>rd</sup> parties! (Facebook makes BILLIONS from this!)
  - Hackers can attack/overcome 2FA, too! (More on this in a moment...)



# Your phone might get hacked first

- “SIM Swapping” attack – Takes over your cellphone 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, of course, are two of the Two-Factor Authentication mechanisms!



# 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 on every website)
  - Correctly answer your “Security Questions” (using your social media posts!)
  - Compromise the website, steal the password database, crack it offline!
  - Lock you out of your account on purpose, to make you use your 2FA (which they then intercept - covered in another slide)



# You might get hacked - “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, then ask you to read it back to them “for verification purposes”
      - *THIS WOULD CONSTITUTE A “LIVE” ATTACK!*
  - Within an email – They get you to click on a link in the email
    - The link takes you to their fake website
    - Looks just like the real website
    - They trick you into typing your real password into their fake website
    - Now they have your password!



# More “dirty-little-secrets”...

- Hacker “shortcuts”, continued...
  - Cracking just one password from a website “unsalts” the rest!
    - Highly technical, but if you hear “salt”/”salted” with regard to passwords, understand that this can be reversed/defeated
  - Amazon Web Services (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”, computers are “electronic locksmiths”
  - Hiring a locksmith is easy (even 24/7/365!)
  - Hiring a “password locksmith” is easy, too
    - Most-popular-password lists are online (covered earlier)
    - Can use online services – submit a “hashed” password, wait a bit...
      - Uses “Rainbow Tables” – Pre-computed lists of hashes and their corresponding plain-text passwords – to spit out the password in seconds!



# Final “dirty-little-secrets”...

- Hiring a “password locksmith”, continued...
  - Be-your-own “locksmith”
    - “john the ripper”, “Hashcat” – free password-cracking tools
    - Kali Linux, Security Onion, Pentoo – bootable Linux images pre-configured with website and password hacking/cracking tools
  - Cracking-as-a-Service
    - Free – Internet based: “submit-and-wait” (usually less than 5 minutes)
    - Paid – Legitimate tools and websites (very few; be very careful!)
    - Paid – “Underground” services (far more dangerous!)
      - *(I wouldn't, if I were you...)*



# What about Two-Factor Authentication?

- You usually have to turn it on (it's not on by default... yet)
- Most “larger”/”mainstream”/popular websites offer it
- Is 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 you already knew or obtained from a “trusted source” (e.g. bank/credit card statement, bill or receipt, etc.) *NEVER TRUST AN EMAILED LINK!*



