Tohono O'odham Nation

Department of Information & Technology

CYBERSECURITY AWARENESS MONTH 2022

Password Protection

Tohono O'odham Nation
Department of Information & Technology

CYBERSECURITY AWARENESS MONTH 2022

Password Protection

Overview

- Password best practices
- Password vs passphrases
- The importance of protecting your passwords
- Checking if your password and account has been compromised
- MFA
- Password keepers

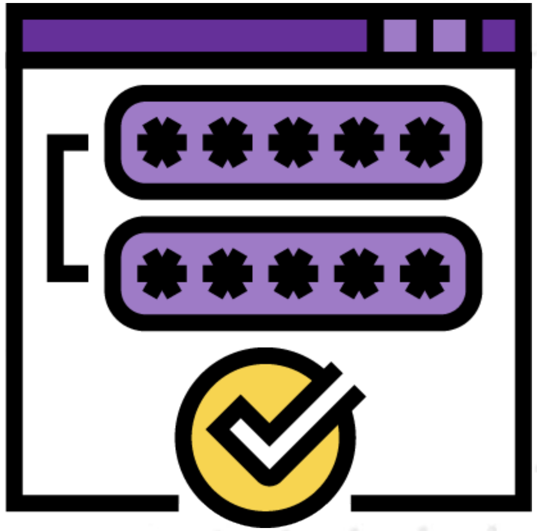
Password Importance

- Your password is the key to accessing your accounts
- If someone gains access to your email - it is a gateway to other personal areas
  - Password resets from other platforms utilize email
  - Financial facilities included
  - Email is used to verify your identity
- Do you use the same password across multiple platforms?
  - Email
  - Social media
  - Bank and credit card sites
- As technology advances, computers are able to guess passwords in seconds as opposed to years, as was the case about 10 years ago
- 8 character passwords are just not safe anymore

Methods Used to Attack Passwords

- Brute Force Attacks- passwords are typed in randomly
- Social Engineering:
  - Phishing emails
  - Passwords not stored securely
- Dictionary Accounts: List of known passwords and account names
- Keyloggers: Malware installed on computer that logs all keys typed in
- Man in the Middle Attacks: This involves the user connecting to rogue access points that records all the communication between two sites, hence, The Man in the Middle
    - Be careful of any Wi-Fi access points you are using

Password Best Practices



- Do not use the same password for multiple accounts
  - Mark Zuckerberg was hacked and used the same passwords across multiple platforms
- Make sure password is complex
- Do not use dictionary words
- Do not use words familiar to you like family name, pet name, birthdate
- Use upper and lower case
- Change passwords periodically
- Try passphrases
- 12 character minimum
- MFA

Passwords To Avoid

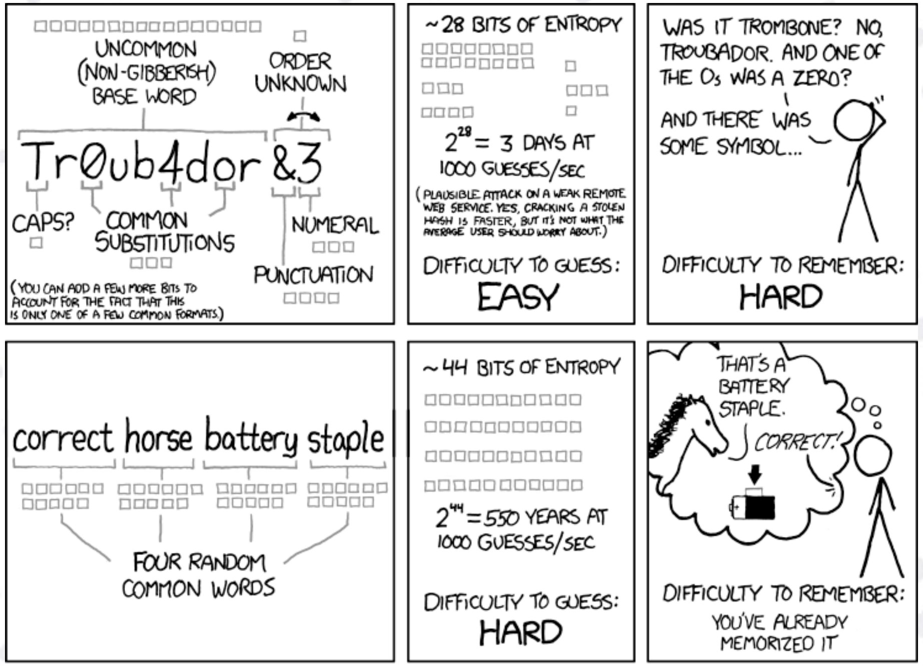
- Other passwords you have to avoid: “sunshine”, “default”, “football”, “computer”, “iloveyou1”, “princess1”, “starwars”, “letmein”, “pokemon”, “batman”, “cookie”

- Basic sequences like “abcd1234”, “qwerty123”, “asdfgh”, “qqww1122", and “1q2w3e4r”

- “password” or its variations like “passw0rd”

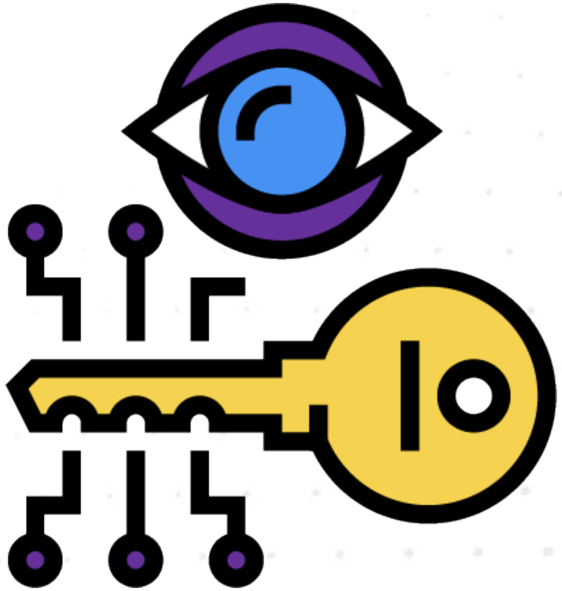
Passphrases

- A combination of words combined
  - Along with special characters and capitalization
- Passwords such as Tr0u13d0R# can be difficult to remember
  - Password is complex enough to meet most requirements


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.

Checking your password



- The sites below allow you to check if your current password has been compromised and the other to generate passwords for you.

- https://haveibeenpwned.com/ : aggregation of compromised passwords
- Password Generator – Strong, Random & Secure Passwords (nexcess.net)

Password Managers

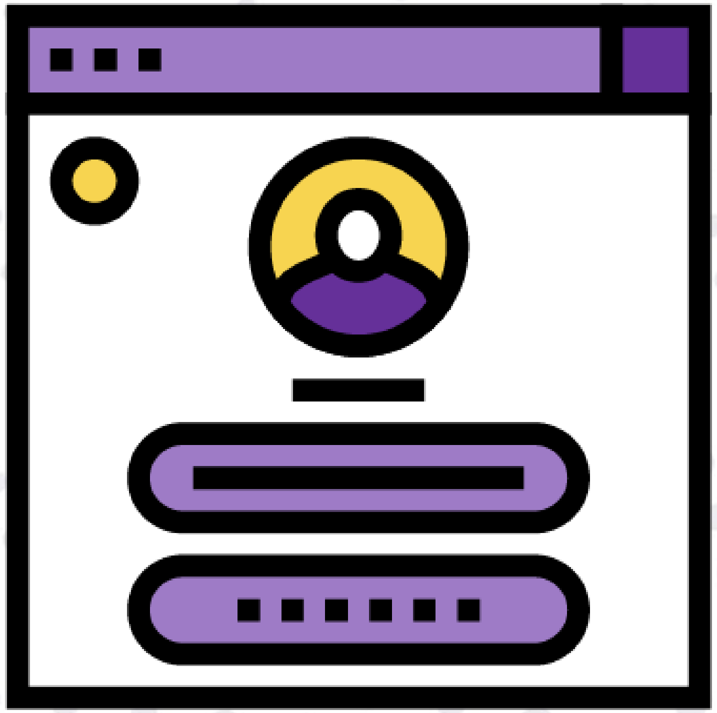
- Allow you to store all of your passwords in one location
- Usually a password to log into the App
- Things to consider
  - Make sure that the passwords are stored encrypted
  - Consider Multifactor Authentication
  - Zero knowledge- the password manager is not storing your main password on the system server
- For more tips go to: Password Managers - National Cybersecurity Alliance (staysafeonline.org)

Multi-Factor Authentication

- More than username and password, it implements an additional step
- Can be:
  - A pin
  - A text or email message to justify
  - An authenticator app
  - A fingerprint or other type of biometrics
- Becoming more available to different apps including
  - Facebook
  - Personal email
  - Shopping apps
  - Bank and credit apps
- Multi-Factor Authentication - National Cybersecurity Alliance (staysafeonline.org)

DoIT Current Password Policy Requirements

- Password complexity requires at least 8 characters
  - At least one special character
  - At least one number
  - At least one letter
  - Capitalization in random areas creates stronger passwords
- Your domain password needs to be reset every 60 days
  - There is no exceptions to keeping the last password
  - There is no exception to not having the password expire
- Considering setting password to a minimum of 12 characters
- Considering MFA for sensitive accounts



Putting It All Together

- As technology progresses, your password management is more important to safeguard
- Your email password is just as important as your bank and financial app
  - Password resets and verification are done through it
- It is important to protect your social media as it is a way to reach your friends and family
- Consider using passphrases
  - Just because it is hard for you to remember doesn't mean a computer with enough computing power can't figure it out.
- Facebook and Instagram offer MFA, as do a lot of applications
  - Consider it whenever possible
- For passwords, technically the longer the better, but consider using passphrases