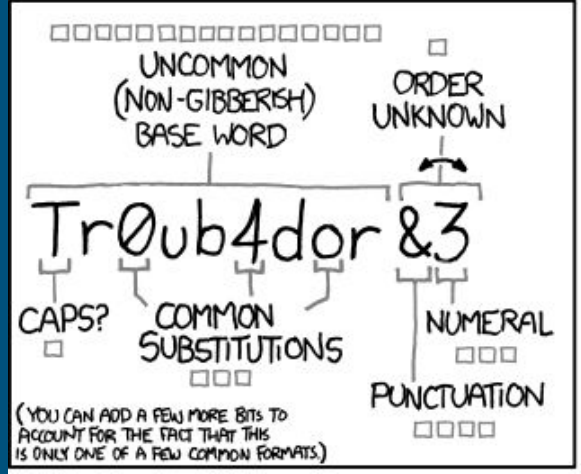
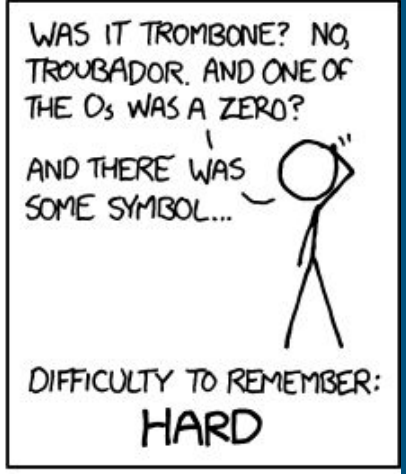
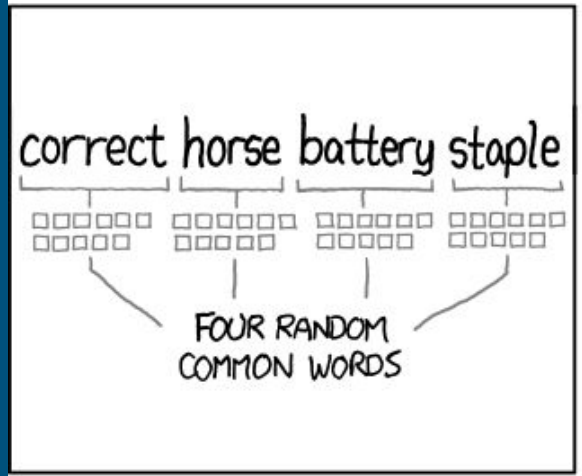
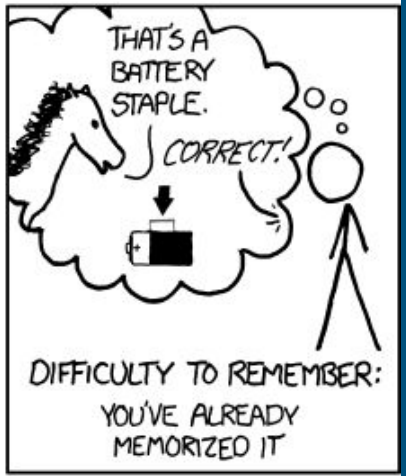
LSIT Training 3/16

Passwords, Encryption, etc. and Why they Matter









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.

BYU General Recommendations

Password Rules

Password rules are based on password length, i.e., the longer the password, the less need for complexity with mixed case letter, numbers, and symbols. Password rules are as follows:

Length	Required Characters
8-11	mixed case letters, numbers, & symbols
12-15	mixed case letters & numbers
16-19	mixed case letters
20+	no restrictions

Additional Requirements:

- It must not be equal to your current password, previous passwords, BYU Netid ID, or password reset answer
- It must not be a single word that appears in the dictionary (English or non-English)
- It must be composed only of characters in the Roman alphabet, numbers, or symbols on the US keyboard. Examples include characters such as # $ % ! @.

SOC Standards:

1.1 - Endpoint Access
2.5 - Server Access
3.4 - Application Access
4.4 - Databases Access
5.2 - Cloud PaaS Access
6.3 - Cloud IaaS Access
7.5 - Email Systems Access

“Review existing accounts and privileges at least semesterly (i.e., fall, winter, spring/summer). Comply with the CES SOC Passwords standard”

CISA-
SECURITY TIP (ST04-002)
NIST-
SP 800-63B

CISA on Storage of passwords `

How to protect your passwords

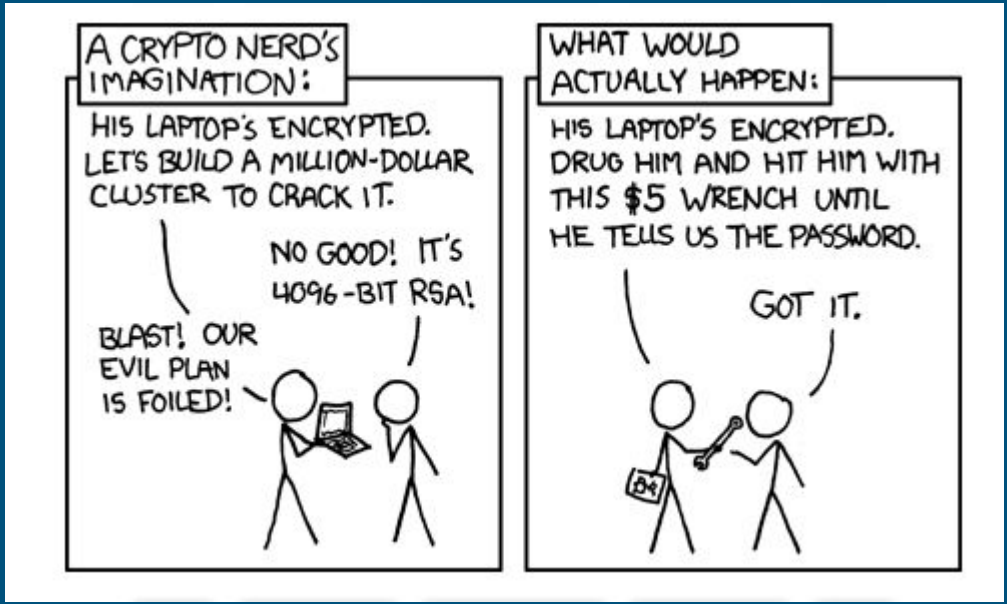
After choosing a password that's easy to remember but difficult for others to guess, do not write it down and leave it someplace where others can find it. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, makes it easily accessible for someone with physical access to your office. Do not tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords. (See Avoiding Social Engineering and Phishing Attacks for more information.)

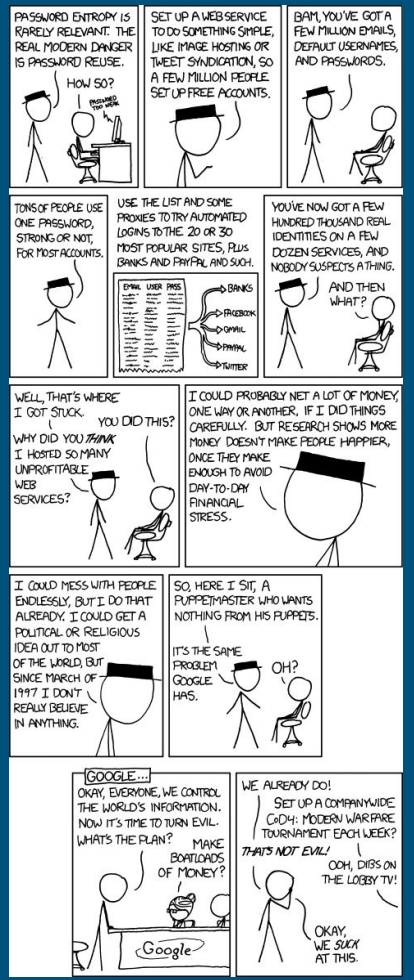
Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password. If you use a password manager, remember to use a strong master password.

Password problems can stem from your web browsers' ability to save passwords and your online sessions in memory. Depending on your web browsers' settings, anyone with access to your computer may be able to discover all of your passwords and gain access to your information. Always remember to log out when you are using a public computer (at the library, an internet cafe, or even a shared computer at your office). Avoid using public computers and public Wi-Fi to access sensitive accounts such as banking and email.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

https://xkcd.com/792/





Hashing Passwords

- Salt
- Protects Data At Rest & Minimizes Storage of Sensitive Data
- At minimum: AES 128, ECC (Curve 25519), RSA 2048.

NEVER NEVER NEVER NEVER MAKE AND USE YOUR OWN METHOD OF HASHING OR ENCRYPTION. JUST DON'T!

You wouldn't perform heart surgery on yourself.

Key Management

- Rotate expired or compromised keys
- Do not store encrypted keys with encrypted data (leaving key in ignition)
- Use approved key storage location or solution

References

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

https://infosec.byu.edu/infosec-standard-minimum-security-controls

https://www.cisa.gov/uscert/ncas/tips/ST04-002