CONTROLS

PASSWORDS

WHY IT MATTERS: GOOD PASSWORD HABITS

Related Services:

AWARENESS TRAINING

USER ACCESS MANAGEMENT

Why? - MAKE PASSWORDS LONG

- ❑ **Math takes time.** Passwords should be stored "hashed" & encrypted. If attackers steal them, they use computers to crack the code. **Short password = easiest & 1st to crack, so they start there.** Long password = longer to crack, buying you time to change your password. **Make passwords 15+ characters as a goal** - letters, numbers, symbols, etc. doesn't matter, just use 15+ characters. *Pro Tip*: phrases work really well.

Why? - MAKE PASSWORDS UNIQUE

- ❑ **One good breach deserves another.** Remembering 1 password is easier that remembering a lot. But, if an attacker steals & cracks your password, then breaches your account or device, chances are good they'll try it on your other accounts & devices. **Use different passwords for each account and device** to limit the damage.

Why? - STORE PASSWORDS SECURELY

- ❑ **Attackers will find your unencrypted password spreadsheet of passwords with automated scanners.**
- ❑ TOOL: Password Managers = apps that create long, random passwords & remember them for you. Just choose a LONG, UNIQUE main password & use two-factor authentication. Yes, it's the jackpot for an attacker, but these companies bet their livelihood they can protect your passwords better than you can.
- ❑ TOOL: Notebook. Simple, effective. You'll know if it's gone & then can change all passwords.
- ❑ Good habits = followed habits. Have a system to create & securely store long & unique passwords? Carry on.

Why? - CHANGE DEFAULT PASSWORDS

- ❑ **Easy targets.** Devices like routers, bluetooth devices, etc. come with default passwords. Attackers scan large swaths of the Internet with tools that find devices with unchanged, default passwords. Since **default passwords are either A. very simple** or **B. published on the Internet**, attackers gain access in seconds (or less). Change your default passwords.

When to Worry

- ❑ **Passwords in the clear? Better fear.** Companies *should* store your password "hashed" & encrypted, using math to garble your password into nonsense so if an attacker steals their database of passwords, they have to spend a lot of time "cracking" them with big computers. No encryption or hashing = easy street for an attacker.
  - ❑ **What to do?** Check the company's "**Terms of Use**," "**Privacy**," or "**Security**" page(s); they usually explain how they store your info. Still can't find it? Google: "**[Company] password storage**."
  - ❑ Enable two-factor authentication as a backup.

INCIDENT RESPONSE: CHANGE THAT PASSWORD

- ❑ A social media company was breached & someone's gotten into your account. Change your password immediately to lock them out, then enable two-factor authentication.