Educational Resource
Password Guide

PCS

ALWAYS ON. ALWAYS CONNECTED.
YOUR 24/7 TECH PARTNER.

Password Best Practices

Hackers harvest and sell corporate and personal passwords for financial gain and other illegal undertakings. 80% of hacks involve the theft or reuse of employee passwords. This list outlines some of the fundamental password security best practices that should be followed:

• Passwords should be at least 14 characters long and use a mix of uppercase and lowercase letters, symbols, and numbers. Consider using the Mnemonic method that creates a difficult password that's easy for you to remember by taking your favorite quote and using the first letter of each word as well as punctuation.

For example: *"Technology will never replace great teachers, but technology in the hands of great teachers is transformational."* becomes: "Twnrgt,btithogtit."

• Avoid recycling the same password across multiple accounts. This prevents a hacker from accessing multiple accounts if they manage to get your password from a data breach.

• After 90 days, change your passwords across all accounts. Keeping track of changing passwords can be a big challenge for some. Solve this by using a password manager app which functions as a digital notebook to keep track of each password. Never write your passwords on a piece of paper next to your computer!

Who is PCS?
Much more than a leading managed IT services company, PCS is built on a foundation of friendly, helpful best-in-class customer service since our start in 2000.

PCS supports highly satisfied customers within numerous industries across the USA including: Small Business, Non-Profits, Accounting, Law, Medical, Insurance, Education, Engineering, Manufacturing, and more.

Our team of experts stand ready to help solve your technology problems. Contact PCS today to discuss your unique IT goals and needs.

www.pcsflorida.com

PCS Florida:
Lakewood Ranch, FL
info@pcsflorida.com

PCS

Password Best Practices continued

• Avoid using birthdays and names of your spouse, children, or pets as passwords as these can be found relatively easily in social media profiles. Also, avoid using real words within passwords as hackers can deploy dictionary attacks which systematically throws every word in the dictionary against your account's login.

• It seems like a week doesn't go by without a company announcing a hack. Use tools like Mozilla's Firefox Monitor, Google's Password Checkup tool, or the website "Have I Been Pwned" to see if your passwords have been identified as compromised.

• Always secure your phone with a fingerprint or facial recognition software.

• Implement MFA (Multi-factor Authentication) which prevents hackers from accessing your accounts even if they crack your password. With an MFA in use, you will be contacted to approve a login before accessing an account.

When it comes to hackers, no digital account is 100% safe. However, following these best practices will go a long way toward keeping your finances and information safe.

www.pcsflorida.com