BEST PRACTICES FOR

PASSWORDS

1 CREATE LONG PASSPHRASES

Create passphrases by combining a few words from a favorite song or quote. Use uppercase letters, lowercase letters, numbers and symbols with at least 9 characters total. Vary the passphrase for each account to increase security.

CYBER AWARENESS TRAININGS 2

Digital threats continue to rise and human error is the main cause of cyberattacks. Attend a PCA training for insights into common threats, refresh your policies and remain compliant, and identify vulnerabilities so you can act before disaster. You can also utilize our partnership with KnowBe4, a leader in cybersecurity awareness, to sign up for Phishing Simulations. We will regularly test your employees by sending fake emails that look like they're coming from a real hacker. We provide the results and suggestions to help keep your team vigilant.

3 ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires you to provide verification factors to gain access to your account. Rather than simply entering your username and password, it will prompt you to use a PIN, a confirmation on your smartphone, or even a fingerprint. WatchGuard AuthPoint MFA will stop 99.9% of hacks!

4 REGULARLY CHECK YOUR ACCOUNTS

The National Institute of Standards and Technology (NIST) recommends organizations utilize services like Dark Web ID to scan for accounts and passwords stolen in previous breaches.

www.pcatg.com | info@pcatg.com | 716.632.5881