While there is a wide variety of opinions over what constitutes a

**10 THINGS YOU CAN DO TO INCREASE PASSWORD SECURITY**

1. Always keep information security top-of-mind.
   - Pithiness known as social engineering. A technique cybercriminals use to trick users information over the phone or in an email, enticing passwords through hooks to convince victims otherwise overwhelming because some other information to respond to hints. victims, such as hints to their headstones, and/or downloading fake attachments.
   - Shoulder Surfing - Watching you enter your password or using a cellphone or even a hidden camera to record password entry.
   - Guessing - Sometimes people try common user passwords or publicly available public locations.
   - Intercepting passwords over unsecured Wi-Fi at airports, coffee shops, hotels, restaurants, etc.
   - Installing physical key loggers or key logging software on devices.
   - Scouring devices and networks for unencrypted passwords.
   - Computerized decryption - Techniques trying every possible combination of numbers, letters, and special characters until a password is discovered (also known as Brute Force Attacks).

2. Point-of-sale (POS) terminals, specialized hardware, desktops, laptops, tablets, smartphones, software, routers, switches, etc. can be accessed from the local area network or any other network connected through Internet to these devices or networks.
   - Computerized decryption - Techniques trying every possible combination of numbers, letters, and special characters until a password is discovered (also known as Brute Force Attacks).
   - Searching devices and networks for unencrypted passwords.

3. Passwords keep information private and financial accounts secure by preventing unauthorized access.
   - Passwords must be treated as private, confidential information.

4. Passwords are private; don't share your passwords with anyone.

5. Use company approved technical solutions for secure password management.

6. Password complexity correlates directly with password security.
   - The stronger the password, the better the chance it will stay safe.
   - The stronger the password, the better the chance it will stay safe.
   - The stronger the password, the better the chance it will stay safe.
   - The stronger the password, the better the chance it will stay safe.

7. Change your passwords regularly.
   - Every 90 to 180 days and immediately upon suspicion or detection of a breach.
   - Every 90 to 180 days and immediately upon suspicion or detection of a breach.
   - Every 90 to 180 days and immediately upon suspicion or detection of a breach.

8. Search engine use.
   - Search engine use.
   - Search engine use.
   - Search engine use.

9. Routinely change passwords when you change a disposal of computing devices.

10. Remove all information from computing devices prior to disposal.
   - And remember, strong passwords. Take the added step of immediately changing your passwords on the replacement devices.

---

**Recommendations: 10 Best Practices for Change default administrator passwords IMMEDIATELY upon installation for all electronic devices at work and at home.**

**Password Information:**

- **Use unique passwords for critical applications.**
- **Change default administrator passwords.**
- **Monitor passwords.**
- **Secure password storage.**
- **Regularly update security measures.**

**Password Security Guidelines:**

- **Password complexity correlates directly with password security.**
  - The stronger the password, the better the chance it will stay safe.

**Password Strengths:**

- **Minimum 8 characters including a number, a lowercase letter, and at least 1 uppercase letter.**
- **Minimum 12 alphanumeric characters.**
- **At least 12 alphanumeric characters.**
- **At least 12 alphanumeric characters.**

**Password Complexities:**

- **Simple passwords (eee, 123, etc.)**
- **Weak passwords (short, one word, or repetitive).**
- **Strong passwords (complex, unique, unpredictable).**

**Password Management:**

- **Use password managers.**
- **Use two-factor authentication.**
- **Use strong encryption.**

**Password Storage:**

- **Only store encrypted passwords on your electronic devices.**
- **Never store unencrypted passwords in email.**
- **Never store unencrypted passwords in email.**

**Password Security Measures:**

- **Implement a password policy.**
- **Use strong encryption.**
- **Use firewalls, anti-virus, and anti-spyware software such as McAfee®, Norton®, Kaspersky®, Windows Defender, etc. for real-time protective monitoring.**

**Password Security Challenges:**

- **Improper password storage.**
- **Improper password storage.**
- **Improper password storage.**

**Password Security Tips:**

- **Use a different password for each site.**
- **Use a different password for each site.**
- **Use a different password for each site.**

**Password Security Implications:**

- **Password security is critical.**
- **Password security is critical.**
- **Password security is critical.**

**Password Security Metrics:**

- **Password complexity correlates directly with password security.**
  - The stronger the password, the better the chance it will stay safe.

---

**Disclaimer:**

This document is provided for informational purposes only and does not constitute legal or professional advice. Users should consult with a professional advisor or legal counsel for specific advice regarding their particular circumstances.