Protecting Your Business:

Is Your Password Policy Putting You at Risk?

Password Security: What You Need to Know

Cybercriminals don't need to "hack" you, they just log in.

Stolen or reused passwords are one of the most common ways attackers break into systems, especially when users recycle passwords across multiple services.

---

5 Key Ways to Strengthen Password Security

1 Use Unique Passwords for Every Account

If a password is leaked in one breach, attackers will try it everywhere. Reusing passwords means one compromised account can lead to a full business compromise.

2 Switch to Passphrases Instead of Short Passwords

Longer passwords are far more secure. Example: CoffeeTablePurple42! is easier to remember and harder to crack than Myp@ss123.

3 Store Passwords Safely

Using a secure password manager helps your team store strong, unique passwords without having to remember them all. Avoid spreadsheets, shared documents, or browser-stored passwords.

4 Turn On Multi-Factor Authentication (MFA)

Even the strongest password can be stolen, MFA adds a critical second layer. We recommend enforcing MFA on email, remote access, admin accounts, and cloud services.

5 New Technologies: Passkeys

Passkeys are the next evolution in authentication, more secure and easier to use than passwords. They use biometrics or device-based approval instead of something you have to remember. While adoption is still growing, we're monitoring it closely for future rollout options.

What Cortec Recommends

- We help our clients enforce strong password policies and MFA across all systems.
- We can advise on secure password manager options for teams.
- We'll help you prepare for future passwordless tech like passkeys.

Get in touch with the Cortec team and we'll help you assess, improve, and maintain security across all devices.

sales@cortecit.co.uk - 020 8467 9222