Beyond “P@ssword123”: A Guide to Passwords and MFA

A Quick Guide for Staff – Provided by Alpha IT Solutions

Introduction: The Game Has Changed

Cybercriminals now use AI-driven tools that can crack short, complex passwords in seconds. To stay secure, we must shift our focus from **complexity** (symbols and numbers) to **length** and **multi-layered identity protection**.

1. Length Over Complexity: The Power of the Passphrase

Predictable substitutions (like replacing ‘a’ with ‘@’) are easily anticipated by hackers. The new gold standard is the **Passphrase**.

- **What is it?** A string of 4–5 random, unrelated words.
- **Example:** Blue-Elephant-Skating-Kitchen
- **Why it works:** It is much easier for a human to remember, but significantly harder for a computer to "brute-force" guess due to its length.
- **Password Fatigue:** Do not change your password unless you suspect a breach. Frequent forced resets often lead to weaker password choices.

2. Multi-Factor Authentication (MFA): The Second Deadbolt

If your password is the key to your front door, MFA is the security guard standing behind it. Even if a hacker steals your password, they cannot gain access without your second "factor."

- **Good:** SMS text codes (vulnerable to 'SIM swapping').
- **Better:** Authenticator Apps (e.g., Google or Microsoft Authenticator). These generate time-sensitive codes that do not travel over a cell network.
- **Best:** Hardware keys (e.g., YubiKey) or **Passkeys**. These use biometrics and cryptographic handshakes that are immune to phishing.

3. Let a Machine Do the Heavy Lifting

Memorising unique, long passwords for over 100 accounts is impossible.

- **Use a Password Manager:** Tools like Bitwarden or 1Password generate and store un-crackable passwords for you.
- **The Master Key:** Your only job is to create one incredibly strong passphrase for the manager itself—and enable MFA on it immediately.

4. The Future is Passwordless: Passkeys

Passkeys allow you to log in using the same biometric check (FaceID or Fingerprint) you use to unlock your phone. They are faster, more secure, and since there is no "password" to steal, they are virtually immune to phishing attacks.

"Staying secure isn't about being a tech genius; it's about being intentional."

For technical assistance, please contact the Alpha IT Solutions support team.

Call: +353 (0)23 881 0061 | **Email:** support@alphait.ie

Scan Me