



Password Security Guide for Staff

Keeping the Organisation Secure

by Calder IT

Why Passwords Matter

Cyber attacks often start with something simple — a weak or reused password.

Even with modern security tools, passwords are still one of the easiest ways for attackers to break into systems.

In fact, **97% of identity-based attacks target passwords**, often by trying common passwords across many accounts. This puts every organisation at risk, regardless of size.

The good news is that a few small changes can significantly improve security for everyone.

What Is a Password Spray Attack?

A password spray attack happens when an attacker:

- Tries **one or two common passwords**
- Across **lots of different user accounts**
- Instead of repeatedly attacking one person

This helps them avoid account lockouts. If even one account is breached, they may be able to access emails, files, or systems.

Three Things You Can Do to Stay Secure

1. Use a Password Manager

A password manager:

- ✓ Creates **strong, unique passwords** for each system
- ✓ Stores them securely
- ✓ Prevents password reuse

This means you only need to remember one strong master password — the rest are handled safely for you.



Password Security Guide for Staff

2. Use Passphrases, Not Short Passwords

If you need to create or remember a password, use a **passphrase**.

A good passphrase:

- ✓ Is **long**
- ✓ Is easy to remember
- ✓ Uses several words together

Example:

✗ *Password123!*

✓ *HalifaxHorsesRunFastAcrossFields*

Longer phrases are much harder for attackers to crack.

3. Always Use Multi-Factor Authentication (MFA)

MFA means you'll be asked for:

- ✓ Your password **and**
- ✓ Something else (such as a phone app or code)

Even if someone steals your password, MFA can stop them getting in.

Key Takeaways

- ✓ Don't reuse passwords
- ✓ Use a password manager
- ✓ Choose passphrases over short passwords
- ✓ Enable MFA wherever it's available
- ✓ Stay alert to suspicious emails or login requests

Cyber security isn't about catching people out — it's about working together to keep systems and data safe.

If you have questions or need help, contact your IT support team.