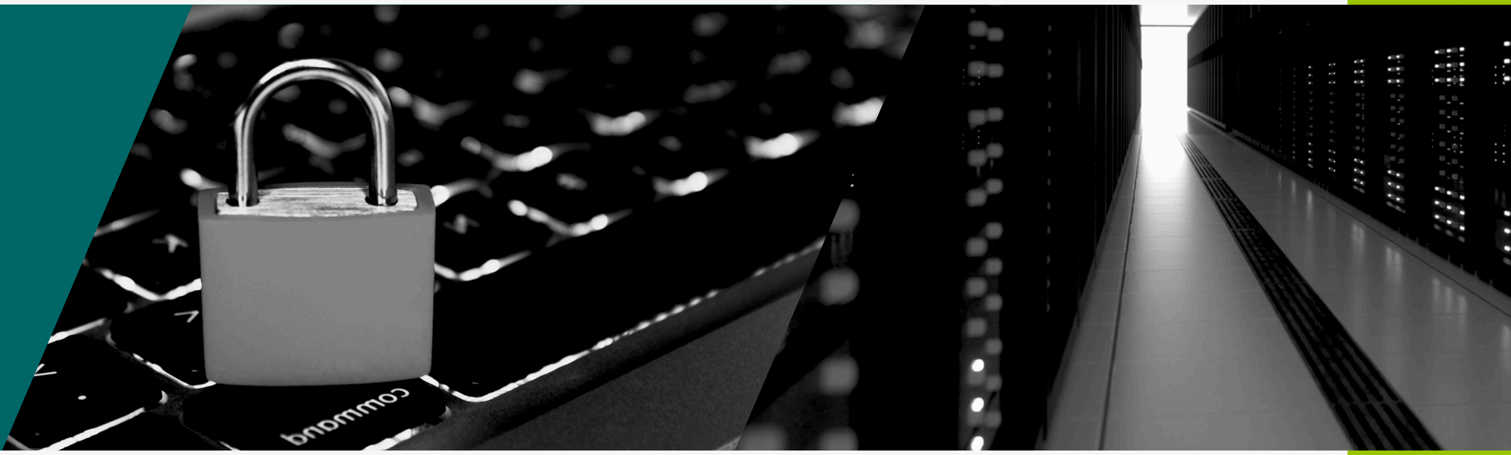
Password leaflet



Brief overview:

What is good password management?

▶ Contains at least 16 characters & mixture of upper and lower case letters, numbers and special characters

▶ Do not reuse passwords (**password manager**) and do not use the "**Save password**" function of applications (e.g. web browsers)

▶ **2-FA** recommended where possible, especially for security-critical applications or system accounts with special rights, e.g. Admin

IT security for SMEs
& the public sector

☎ +41 31 508 76 20

www.linkyard.ch

Junkerngasse 39,
3011 Bern, Switzerland

More security for your passwords - here's how it works in detail

Password checklist

- ✓ Variety is crucial (letters, numbers, special characters)
- ✓ Do not use common words or patterns (“password123”, “qwerty” or “123456” are insecure)
- ✓ Do not use any personal data (avoid date of birth, names, telephone numbers)
- ✓ Passphrases are a good alternative, e.g. “Fall2025TeamProjectStart!”
- ✓ Use each password only once
- ✓ Use a professional password manager, e.g. LastPass
- ✓ Regularly check whether passwords have been leaked
- ✓ Activate multi-factor authentication (MFA) for all important accounts
- ✓ “Save password” functions of browsers/apps are convenient but risky. They offer an easy target for attackers
- ✓ Secure emergency access (keep backup codes safe)

Bonus: Passkeys
The future of passwords

Passkeys replace passwords with a **secure crypto-graphic key pair**. One key remains on the device, the other is stored on the server. You can log in using your **fingerprint, facial recognition** or **PIN** - without a password.
Passkeys are **more secure** as they cannot be stolen or tapped by phishing. They only work with the registered website or app. Major companies such as Apple, Google and Microsoft already support them.

Conclusion: Easier, more secure and more convenient than passwords 🔐

IT security for SMEs
& the public sector

☎ +41 31 508 76 20

🌐 www.linkyard.ch

📍 Junkerngasse 39,
3011 Bern, Switzerland