

Passwords and Two-Factor Authentication in an SME

Almost nobody guesses a password. Attackers get it from a breach on some unrelated website, and it works because the same password was reused on the work email account. That is the most common way into a company inbox, and from there into invoices, client data and other credentials.

Length beats forced complexity

Requiring capitals, symbols and a change every 90 days does not make passwords stronger: it gets them written on a sticky note or repeated with a tiny variation. A long, unpredictable phrase, unrelated to the company or to personal details, resists guessing better and is easier to remember. Change a password when there is a sign it leaked, not on a fixed schedule.

A password manager for everything shared

Shared accounts (social media, tools, suppliers) are the weak point: they circulate in chat messages and stay unchanged for years. A password manager generates and stores a unique password per service, shares it without ever typing it into a message, and lets you revoke

access when someone leaves without changing the password for everyone else.

Two-factor authentication, in the right order

Turn it on first for email and remote access, the doors that open everything else. Then for admin accounts. Then for the rest. SMS codes are the weakest second factor, because they can be intercepted; an authenticator app or a physical security key protects better. Even so, SMS is far better than nothing.

A rollout that avoids a revolt

- Start with the people who hold the keys: leadership, IT administration, whoever handles email and finance.
- Explain the reason before the rule: the real risk convinces more than an order.
- Set a reasonable deadline and help anyone who struggles with the app.
- Decide in advance how access gets recovered if a phone is lost, so nobody stays locked out for a day.

Want to know if your company is truly protected?

Ciphraverse helps SMEs turn technical findings, regulatory pressure and client questionnaires into clear security decisions.

Explore services on ciphraverse.com



Ciphraverse Checked

The visible sign of a serious commitment to security.