CYBERSECURITY 101 · eBuilder Security

Cyber Hygiene

Most breaches do not come from clever new attacks. They come from the basics left undone. Here is what good cyber hygiene looks like, and the one habit that stops the most attacks.

WHAT IT IS

Cyber hygiene is the set of routine habits that keep your systems, accounts and data secure. Like personal hygiene, it is a handful of simple things done consistently rather than one big project. Patching, strong passwords, multi-factor authentication, backups and controlled access are the core. It is the highest-value security work most organisations can do, because almost all successful attacks exploit poor hygiene rather than anything sophisticated.

WHY IT MATTERS

About 60%

of breaches involve the human element, usually phishing or weak credentials.

Verizon DBIR, 2025

More than 99.2%

of account compromise attacks are blocked by multi-factor authentication.

Microsoft, 2024

4.44 million USD

global average cost of a data breach.

IBM, 2025

WHAT HAPPENED

In August 2025 a ransomware attack hit Miljödata, a Swedish supplier whose HR software is used by around 80% of the country's municipalities. Attackers did not need to breach each council, only the one supplier they all relied on. Swedish authorities confirmed 164 municipalities and four regions were affected, out of 290 municipalities, with sensitive records exposed and later published online. (The Record, 2025)

RED FLAGS TO WATCH FOR

You can tell hygiene is slipping before an attacker does. Watch for these.

- Software and systems running past their update deadlines, sometimes for months.
- Accounts protected by a password alone, with no multi-factor authentication.
- Old employee logins and admin rights nobody has switched off.
- Backups that exist on paper but have never actually been restored.
- Suppliers with access to your data whose security you have never checked.

THE ONE RULE THAT STOPS IT

Turn on multi-factor authentication everywhere, so a stolen password on its own is never enough to get in.

THEN BUILD THE HABIT AROUND IT

- Patch software and firmware on a schedule, and faster for anything internet-facing.
- Keep an up-to-date inventory of your devices, software and suppliers.
- Use a password manager and long, unique passwords for every account.
- Keep tested backups, with one copy offline or immutable.
- Run regular, role-based security awareness training.

MYTHS AND FACTS

MYTH

We are too small to be a target.

FACT

Small organisations are targeted because their hygiene is often weaker. Attackers scan for easy entry, and size is no protection when the door is unlocked.

MYTH

A strong password is enough on its own.

FACT

Strong passwords still leak or get phished. Multi-factor authentication is what stops a stolen password from working, and Microsoft reports it blocks more than 99.2% of account compromise attacks.

MYTH

Cyber hygiene is the IT department's problem.

FACT

Most breaches involve people outside IT, through phishing or weak passwords. Hygiene is a shared habit, and under NIS2 it is a board-level duty.

THE LEGAL DUTY

In the EU, cyber hygiene is now law. NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, requires basic cyber hygiene practices and cybersecurity training in Article 21(2)(g), with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based security awareness training and phishing simulations that build these habits and keep them consistent. Read the full guide at the link below.

Read the Full Article →