

OSINT

Open-source intelligence is how attackers research your people from public information, long before they send a single email. Here is the risk, and the habit that stops most of it.

WHAT IT IS

OSINT, short for open-source intelligence, is the collection of information from publicly available sources such as social media, company websites, public records and leaked data. In cyber security it is the quiet first stage of an attack. It breaks no system and sets off no alarm, which is exactly what makes it so hard to stop.

WHY IT MATTERS

60%

of intrusions into EU organisations began with phishing, the lures OSINT makes convincing

ENISA Threat Landscape, 2025

\$3.05bn

lost to business email compromise, reported to the FBI in 2025

FBI IC3, 2025

>80%

of observed social engineering activity now uses AI-assisted phishing

ENISA, 2025

WHAT HAPPENED

In 2023, the group tracked as Scattered Spider profiled an employee of MGM Resorts from public sources, then called the IT help desk posing as that person and had a password and MFA factor reset. MGM told regulators the incident would cost around 100 million dollars for the quarter. (MGM Form 8-K and a joint CISA and FBI advisory, 2023.)

RED FLAGS TO WATCH FOR

The reconnaissance is invisible. The attack it feeds is not.

- Urgency paired with a demand for secrecy
- A request that skips the normal process, such as a payment or a password reset
- A pretext that uses real names, your manager or a live project
- A channel that does not fit, like an email about money from someone who always calls
- A web address that is almost right, with an extra word or a swapped letter

THE ONE RULE THAT STOPS IT

Verify any unusual or urgent request on a second channel you already trust, never the contact details in the message itself.

THEN BUILD THE HABIT AROUND IT

- Audit your own public footprint the way an attacker would

- Keep software versions and internal tooling out of job adverts
- Give the help desk an identity check an attacker cannot look up
- Use phishing-resistant MFA so a stolen password is not enough
- Make reporting a suspicious message quick and free of blame

MYTHS AND FACTS

MYTH

OSINT is a form of hacking, so it must be illegal.

FACT

It uses only public information, which is what makes it legal, cheap and hard to stop.

MYTH

We have nothing worth researching.

FACT

Names, roles, an email format and one reused password are enough to build a convincing attack.

MYTH

A strong firewall stops reconnaissance.

FACT

It happens on public sites and in breach data, outside your perimeter, so technology alone cannot block it.

THE LEGAL DUTY

Under the EU NIS2 Directive and Sweden's Cybersäkerhetslagen (SFS 2025:1506, in force 15 January 2026), security awareness training is a required measure, and a company's board can be held personally accountable for it.

GET HELP

Train your people against these exact tactics and shrink the footprint attackers rely on.

[Read the Full Article →](#)