

Cyber Fatigue

Staying secure now means more passwords, more prompts and more alerts than people can keep up with. Here is what cyber fatigue is, why it causes breaches and the one habit that fights it.

WHAT IT IS

Cyber fatigue is the weariness that sets in when the demands of staying secure outpace what a person can manage. In staff it shows as security fatigue, so they reuse passwords and approve prompts without thinking. In security teams it shows as alert fatigue, a numbness to the flood of alarms. Attackers count on both.

WHY IT MATTERS

~60%

Of data breaches involve a human element, the fatigue-prone link attackers target.

Verizon DBIR, 2025

40 million

Payment-card records stolen from Target after its team did not act on alerts that flagged the malware.

US Senate Commerce Committee, 2014

99%

How SOC analysts described their false-positive alarm load in a University of Oxford study, the root of alert fatigue.

University of Oxford, 2022

WHAT HAPPENED

In September 2022 an attacker used an Uber contractor's stolen password and then flooded the contractor's phone with multi-factor prompts. After a WhatsApp message posing as Uber IT, the worn-down contractor approved one and the attacker reached internal systems. Uber linked the activity to the Lapsus\$ group. (Uber security update, 2022)

RED FLAGS TO WATCH FOR

Fatigue is quiet, so watch the behaviour, in your people and in the alert queue.

- Multi-factor prompts you did not start, arriving in a burst.
- Warnings and prompts approved or clicked through without being read.
- A growing backlog of security alerts no one has investigated.
- Detection rules muted or switched off to quiet the noise.

THE ONE RULE THAT STOPS IT

If a security prompt arrives that you did not start, deny it and report it. Never approve one just to make it stop.

THEN BUILD THE HABIT AROUND IT

- Turn on number matching, or move to phishing-resistant keys for important accounts.
- Cut the number of security decisions staff face day to day.

- Tune detections so the alerts that remain are worth acting on.
- Give the security team enough capacity, in-house or managed, to answer real alerts.

MYTHS AND FACTS

MYTH

Cyber fatigue is a personal weakness.

FACT

It is a predictable response to overload. NIST found ordinary users slide into resignation and decision avoidance when asked to make more security choices than they can manage.

MYTH

Multi-factor authentication makes us safe from this.

FACT

Push-based multi-factor can be defeated by fatigue. Attackers flood a user with prompts until one is approved, which is why CISA recommends number matching or phishing-resistant keys.

MYTH

If an alert fires, someone will act on it.

FACT

Not if the team is numb to alarms. At Target in 2013 the warnings fired and went unanswered, and around 40 million card records were stolen.

THE LEGAL DUTY

Security awareness training and continuous monitoring are legal duties under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based security awareness training and managed detection and response that cut the decisions and the noise behind cyber fatigue. Read the full guide at the link below.

[Read the Full Article →](#)