CYBERSECURITY 101 · eBuilder Security

Credential Stuffing

How attackers turn one leaked password into account takeover at scale, and the controls that stop it.

WHAT IT IS

Credential stuffing is the automated testing of stolen username and password pairs against login pages. The passwords come from other companies' breaches, and reuse means one old leak can open many accounts. A business feels it as account takeover, fraud and, where personal data is exposed, a reportable breach.

WHY IT MATTERS

88%

Of web application attack breaches involved stolen credentials.

Verizon DBIR, 2025

1.1 million

Accounts compromised across 17 companies, most attacks undetected.

New York Attorney General, 2022

GBP 2.31M

UK ICO fine over the 23andMe credential stuffing attack.

UK ICO, 2025

WHAT HAPPENED

In 2023, attackers ran leaked credentials against 23andMe and accessed about 14,000 accounts, roughly 0.1 percent of its users. Through linked-relative features those accounts exposed data on about 6.9 million people. 23andMe's own systems were never breached. The UK ICO later fined it GBP 2.31 million. (UK ICO)

RED FLAGS TO WATCH FOR

Signs your login is under attack:

- A sudden spike in failed logins.
- A surge in account lockouts.
- Sign-ins from many unfamiliar IP addresses and countries.
- Impossible travel on a single account.
- A rise in account-takeover complaints.

THE ONE RULE THAT STOPS IT

Turn on multi-factor authentication across every account, ideally phishing-resistant passkeys. A stolen password alone is then not enough to log in.

THEN BUILD THE HABIT AROUND IT

- Screen passwords against known-breach lists at signup and reset.
- Add bot detection and rate limiting on the login.

- Move toward passwordless sign-in.
- Use unique passwords and a password manager.

MYTHS AND FACTS

MYTH

A strong password protects me.

FACT

Not against credential stuffing. Once a password has leaked elsewhere, attackers replay it as it is.

MYTH

If our systems were not breached, we are not liable.

FACT

23andMe's systems were never breached, yet the UK ICO still fined it GBP 2.31 million.

MYTH

We would notice an attack this big.

FACT

The New York Attorney General found most credential stuffing attacks had gone undetected by the companies.

THE LEGAL DUTY

NIS2 Article 21(2)(j) names multi-factor authentication as a required measure, and Sweden's Cybersäkerhetslagen makes it law. If an attack exposes personal data, GDPR Article 33 requires notifying IMY within 72 hours.

GET HELP

Check whether your credentials are already leaked, and put layered login defences in place with eBuilder Security. Read the full guide at the link below.

Read the Full Article →