Dark Web Monitoring
Employee Onboarding Guide

As part of our commitment to security and privacy, we've implemented a dark web monitoring service. This guide will help you understand what dark web monitoring is, how it works, and how it affects you.



Why is it vital for us to combat dark web threats?

The dark web poses significant threats to our security, primarily through the misuse of stolen user credentials. In this shadowy part of the internet, attackers can buy or sell credentials obtained from internal and third-party data breaches, enabling them to access personal and corporate accounts. This access can lead to further security breaches, financial theft, identity theft, and even corporate espionage.

Stolen credentials are the primary method attackers use to breach a business.
(2023 Verizon DBIR)

50%

of breaches stem from stolen or compromised credentials, like user passwords.
(2023 Verizon DBIR)

62%

of breaches (not involving human error) involved the use of stolen credentials, brute force, or phishing.
(Varonis)

- Helps in early detection of data breaches, reducing potential harm.
- Keeps us informed about our digital footprint and vulnerabilities.
- Helps in complying with data protection regulations.
- Protects our brand reputation by reducing the impact of data leaks.

Dark web monitoring – An additional layer of security

Each of us plays a crucial role in safeguarding against dark web threats. By adhering to security protocols, like using strong passwords and reporting suspicious activities, we can significantly reduce the risk of our data being compromised and ending up on the dark web. To strengthen our resilience, the business has introduced an internal dark web monitoring service to help us protect our business's reputation, and ensure the security of both the company and our personal information.

Our dark web monitoring service – How it works

1 Scan

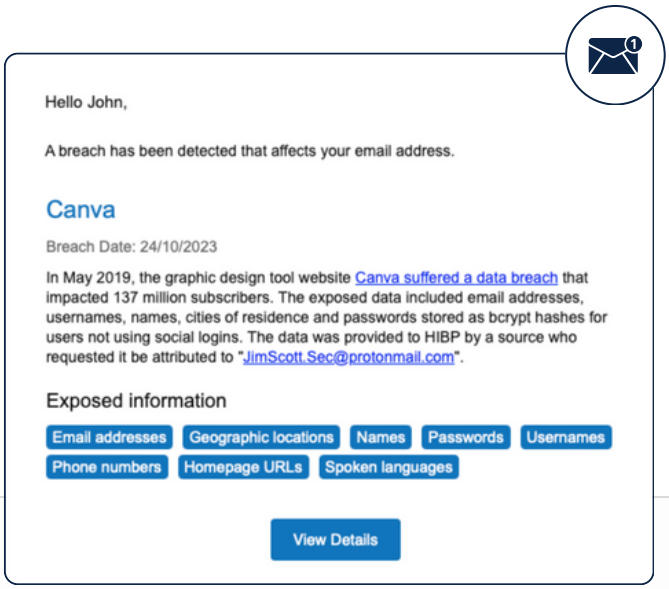
An extensive database of breach sources will be scanned, identifying whether any of your corporate data *(e.g. your business email password)* is present in a data breach.

Ongoing dark web monitoring will then take place, continuously scanning new data breaches to identify whether you are at risk.

Where is breached data often located?

- **Dark web chatrooms** – hidden chatrooms where breaches are discussed
- **Hacking and dump sites** – dark web sites where breached data is shared
- **Hidden theft forums** – hacking communities where breached data is published
- **P2P file leaks** – data leaked through peer-to-peer networks

What data is commonly found? Passwords | Bank Account Details | Addresses | Phone Number | Medica



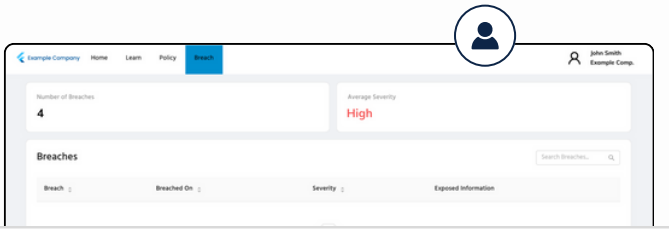
2 Alert

If at any point your data or credentials are found in a breach, you'll receive an **email alert** (example, left) which includes the:

- List of breaches you are affected by
- Source and date of the breaches
- Types of data that are exposed
- Plus, a link to view more details

Your data has been found in a breach, now what?

If you are notified by our dark web monitoring service that your data has been found in a breach, it's important to act promptly to safeguard your information and to reduce your human risk score in your **End User Portal** (example, below).



Here's a few tips on how to reduce your risk:

- **Change passwords:** Immediately update the passwords for any affected accounts. Use strong, unique passwords for each account.
- **Contact financial institutions:** If financial information is involved, promptly contact your bank or credit card company.
- **Secure email accounts:** For compromised email accounts, update your security settings and activate two-factor authentication if not already in use.
- **Monitor financial statements:** Regularly check your bank and credit card statements for any suspicious transactions.