

Dark Web Monitoring

Dark web monitoring is a service that searches for and monitors information found on the dark web. The service looks for stolen and/or leaked information, such as compromised passwords, credentials, intellectual property, and other sensitive data being shared and sold among criminals operating on the dark web. This information can include:

- Credit card details.
- Account credentials.
- PII information (name, address, phone number etc.)

If this information is found, a breach report is generated and the associated employee(s) are notified. Additionally IT is notified so immediate action can be taken if required.

FAQ

Answers to commonly asked questions.

What do I do if I receive a breach report?

Check and see if any of your accounts are at immediate risk of being accessed by an unknown person. If yes, change your password immediately and notify IT. For certain types of reports such as web scrapping unfortunately little can be done other than being vigilant as you'll be at increased risk for identify theft.

IT receives all breach reports and will reach out if concerned. If the breach is considered significant, the affected accounts may be temporary disabled with no notice to you to ensure the security of the company.

How does 1Password determine that a breach has happened?

After a company or individual has been compromised, it's common for the hacker to either:

1. Attempt to sell the information online (usually on the dark web).
2. Publicize the information.

1Password looks for these types of posts and analyzes any information collected. If information related to George & Bell Consulting is found, a breach report is generated.

I recently learned that my personal information was collected. What can I do about it?

Be vigilant as you'll be at increased risk of identity theft with your personal information publicized. Here are a few steps you can take to protect yourself:

- Monitor your credit cards and call the credit card company immediately if anything is amiss.
- Place a credit freeze on your name. This will stop any identity thieves from opening any account that includes a credit check (loans, credit card etc.).
- Don't be truthful when setting up security questions. For example, when asked what city you were born in, lie. (but do document it so you can remember it!)
- Call various providers to see if they can add additional security checks as part of verifying who you are.

If you do become the victim of identity theft, the recommended approach is to:

- notify your financial institution and the local police.
- contact the CRA at 1-800-959-8281.
- report the theft to a credit reporting agency such as Equifax or TransUnion.
- keep records of recent purchases, payments, and financial transactions.
- Call 1-800-O-Canada (1-800-622-6232) for information on how to replace identity cards such as your health card, driver's license, or SIN if necessary.

[More Information](#)

Where can I learn more about this service?

Please visit [1Password's Support](#) site.

What can I do personally if my information is released?

Monitor your credit cards and call the credit card company immediately if anything is amiss. Common signs of identity theft include:

- Receiving an application for credit in your name
Your bank informing you that they have approved/denied your application for a service you never applied too
- No longer receiving a statement and finding unusual purchases.

If extremely concerned, you can place a credit freeze on your name. This will stop any identity thieves from opening any account that includes a credit check (loans, credit card etc.).

- Don't be truthful when setting up security questions. For example, when asked what city you were born in, lie. (but do document it so you can remember it!)

- Call various providers to see if they can add additional security checks as part of verifying who you are.

Revision #6

Created 29 November 2023 17:53:56 by Tyler Rasmussen

Updated 29 November 2023 22:38:51 by Tyler Rasmussen