TECHNAGY IT
empowering you

Dark Web Monitoring

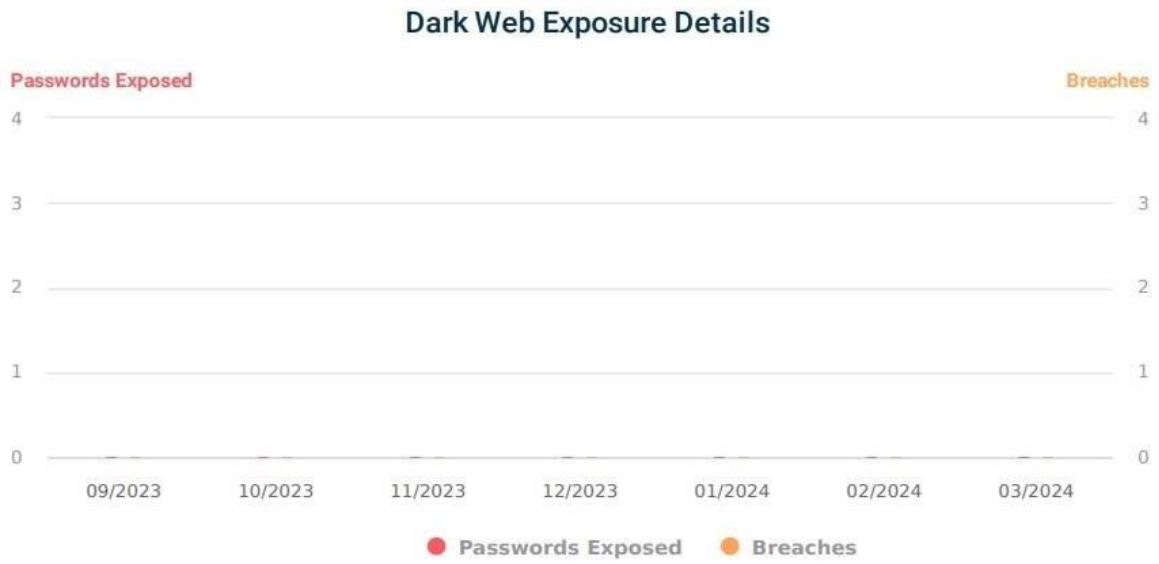
Dark Web Monitoring

Personal information being sold on the dark web is one of the most significant risks that can expose individuals and organizations to vulnerabilities. To safeguard against this, knowing if employees have been involved in any dark web breaches is essential. By being aware of your organization's dark web status, you can take proactive measures, such as securing compromised accounts and remaining vigilant for targeted phishing attempts to protect yourorganization.

- Email Accounts Affected Details
- Dark Web Overview and Current Dark Web Status.
- A summary of all the breached information posted to the Dark Web every month.
- Latest Dark Web Breach Details

Compiled a list of the breaches affecting your domains during the last month. In addition,all Dark Web data from previous months is provided. All exposed data is important butnote the most recent breaches and address them immediately.

Note: This graph has no values, symbolizing that there have been no breaches in the past month.



For: Altera Fund Advisors

Provided By: Technagy

Date: 11/6/2025

Dark Web Status Report

11/6/2025

1. Background Information

What is the Dark Web?

The Dark Web is an anonymous part of the internet where cybercriminals trade stolen information such as email credentials, passwords, and sensitive data. Once compromised, this data is often sold to other bad actors who can exploit it for malicious purposes, including financial fraud, identity theft, or launching targeted attacks. As cybercrime continues to evolve, organizations remain at risk if they are unaware of exposed information, leaving employees and businesses vulnerable to breaches.

Purpose of this Report

This report is designed to provide insights into the risks that Dark Web activity poses to your organization. It includes an overview of global Dark Web trends and highlights any breaches involving your company's email domain. The report also provides actionable recommendations to help you address potential vulnerabilities, mitigate risks, and enhance the security of your employees and organization against future threats.

2. Global Monthly Dark Web Summary

Dark Web Overview

November 2025

The Dark Web remains an active marketplace for cybercriminals, constantly evolving to exploit new vulnerabilities. This section highlights global Dark Web activity, presenting both monthly trends and cumulative data to provide a comprehensive view of breaches worldwide. Use this context to compare global trends with the specific breaches affecting your organization in the following sections.

Exposed Passwords

November 2025	Total-to-date
0	7,026,494

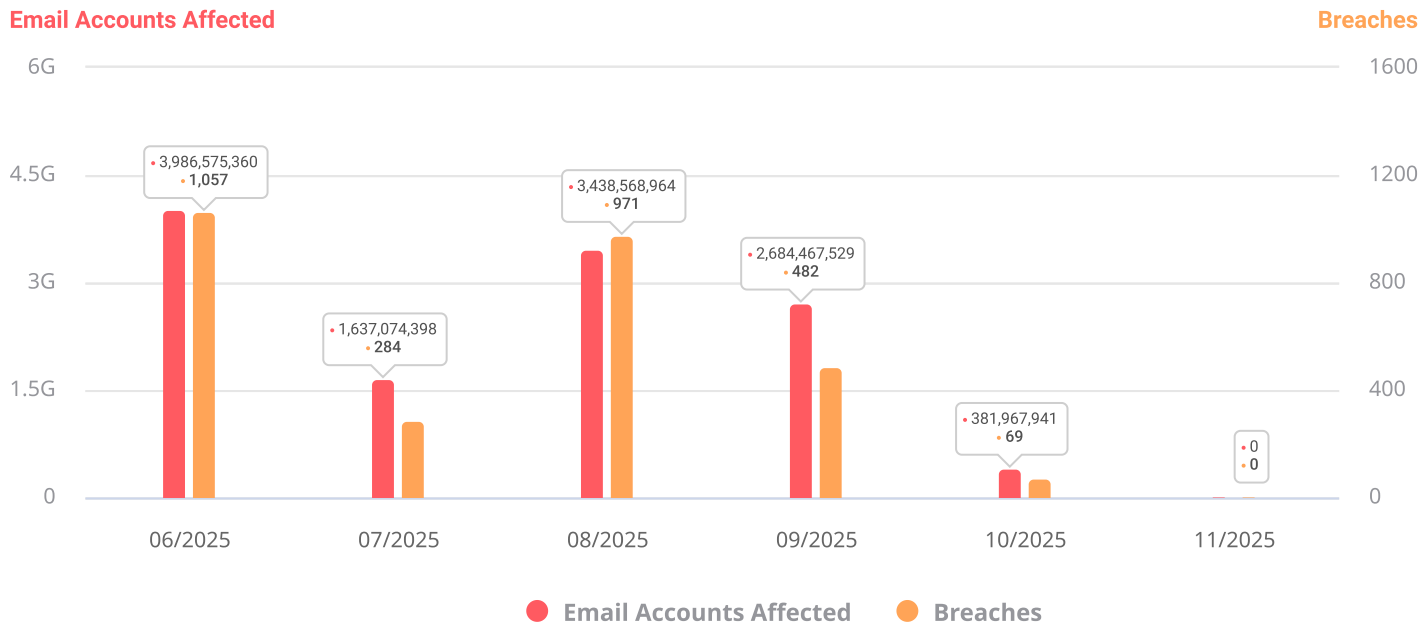
Total Data Breaches

November 2025	Total-to-date
0	8,984,526

Dark Web Trends

Previous 6-Months

Our human operatives are constantly scouring the Dark Web for newly exposed data. Here's a look at what they've uncovered over the past six months. Understanding the previous Dark Web posting trends can help forecast risks.



3. Your Current Dark Web Status

Domains Monitored

1

Exposed Passwords

10

Total-to-date

Total Data Breaches

17

Total-to-date

Overall Risk

High

Exposure on the Dark Web introduces significant risks to your organization. Compromised information such as passwords, email addresses, and other personal details can be leveraged for phishing attacks, unauthorized access, or further breaches. With this report, you have a clear analysis of employee exposures and actionable steps to address vulnerabilities.

It's essential to remain vigilant, even if no breaches are detected for your domains. Breaches can occur at any time, and educating employees on cybersecurity best practices can play a key role in preventing future incidents. Regular monitoring and proactive security measures are your best defenses against evolving threats.

Domains Monitored

alteradevco.com

3. Your Current Dark Web Status

4. Latest Dark Web Breach Details

Below is a list of the 200 most recent breaches. For additional details, please login to the platform: https://portal.breachsecurenow.com

Dark Web Breaches

0

Total-of-Dark Web Breaches

Breaches Remediated

0

Total Breaches Remediated

5. What's the impact?

Breached Passwords

When breached account credentials like email address and passwords become available on the dark web, they can be used to access that account, steal information, or access additional accounts that may use the same credentials.

Spear Phishing

Even if passwords weren't compromised on the dark web, the email address, physical address, or other personally identifiable information can be used to craft specific and convincing phishing emails that could put your business at future risk.

Network Access

If the credentials compromised are the same credentials used to access your business network or sensitive customer information, criminals could use this information for unauthorized access to your network where they can wreak havoc.

6. What happens now?

Someone at your organization has had data exposed on the Dark Web—what does this mean for your business? A third-party data breach involving your employees' business accounts can create serious vulnerabilities. This section outlines proactive steps you can take to address these risks and protect your organization.

How Can I Protect My Employees and My Business?

We understand that discovering your organization's data on the Dark Web can be concerning, but it's an opportunity to take proactive measures. This report is shared to empower you with the knowledge needed to prevent this information from being exploited. We strongly recommend taking the following steps to remediate the risks and protect your organization.

1. 

Update Passwords

Immediately change passwords for all compromised accounts.
Ensure passwords are strong, unique, and not reused.

2. 

Provide Security Awareness Training

Educate employees on cybersecurity best practices, including recognizing phishing emails and understanding scams like spear phishing.

3. 

Limit Business Email Use

Advise employees to avoid using their business email for non-business activities to reduce exposure risks.

4. 

Enable Multi-Factor Authentication (MFA)

Secure accounts with an additional layer of protection to mitigate the risk of unauthorized access.

5. 

Encourage Proactive Monitoring

Ensure you implement continuous monitoring to receive real-time notifications about new breaches on the Dark Web. Encourage employees to periodically check their personal email addresses for potential exposure using reliable tools to maintain comprehensive security awareness.

Have **questions** or want more tips on best practices?

If you have questions on any of these results or how to proactively protect your employees and your business, please feel free to contact us!