Business Dark Web Monitoring

What is the Dark Web and Why Does it Matter to Your Business?

The Dark Web is a concealed part of the internet that is not indexed by standard search engines, existing below the "surface web" that you probably use every day, and requires specific software and knowledge to be able to access and navigate. While it does have legitimate uses, even Facebook and many news sites can be reached on the dark web, it is notoriously known for hosting illegal activities—including the sale of stolen data, intellectual property, customer information, and in the case of this document… username and password credentials.

For businesses, the Dark Web presents a significant risk. Cyber criminals frequently trade compromised passwords, employee email addresses, and sensitive company data obtained through phishing attacks, data breaches or malware infections. Once these details are exposed, attackers can exploit them to infiltrate systems, impersonate users, and orchestrate larger-scale attacks such as ransomware or business email compromise.

In 2024, 26 billion username and password combinations were leaked on to the dark web in the "Mother of all Data Breaches", with billions more records including personal details such as your phone number, address and more also leaked every year.

Unfortunately, many of these records belong to business domain registered accounts, leaving those businesses vulnerable to potential targeted attacks on everything from your social media accounts, to your purchasing accounts, and even banking information. Early detection through a Dark Web monitoring solution can make the difference between a proactive defence to prevent or mitigate these risks, and a catastrophic breach.

Business Benefits of Implementing a Dark Web Monitoring Solution

Early Breach Detection

Dark Web monitoring helps identify leaked credentials and sensitive data before attackers act. This allows your business to take preventative measures—such as resetting passwords or revoking access—before damage occurs.

Protection of Brand Reputation

A data breach can severely harm public trust, ruining your reputation with your existing customers, and alienating prospective customers against trusting your brand to securely manage their data. Monitoring the Dark Web supports your company's due diligence in cyber security, demonstrating a strong commitment to protecting your business, as well as your client and stakeholder data.

Regulatory Compliance

UK GDPR, as well as other industry standard cyber security and data security frameworks (Cyber Essentials and ISO27001) require swift breach detection and response, Dark Web monitoring supports your legal and regulatory obligations to protect personal, business, and client data.

Risk Reduction and Cost Savings

Reports state that the average cyber security breach cost in the UK is £3.4 million. Proactive threat intelligence significantly reduces the likelihood and impact of such events.

Integrating Dark Web Monitoring with Password Policies, SSO and MFA

Dark Web monitoring is most effective when part of a layered cybersecurity strategy. It should not be a standalone tool but work in conjunction with other critical components:

Strong Password Policy

A robust password policy should mandate complex, unique passwords and regular updates. When integrated with Dark Web monitoring, any exposed passwords can trigger automatic resets and user notifications.

Single Sign-On (SSO)

SSO centralises user authentication, reducing the number of credentials in use and lowering the attack surface. When paired with Dark Web monitoring, SSO systems can flag compromised accounts in real-time and enforce secure login processes.

Multi-Factor Authentication (MFA)

MFA adds an essential security layer, requiring users to verify their identity beyond just a password. If credentials are found on the Dark Web, MFA significantly reduces the chances of unauthorised access—even if passwords are exposed.

Dark Web Monitoring & Alerting with TwentyFour

Investing in a Dark Web Monitoring solution is not just a technical safeguard from evolving threats, it is a strategic decision that enhances your business resilience, protecting your employees, your data, and your business reputation.

Our Dark Web Monitoring service, when linked with wider business Password Policies, including SSO & MFA, forms a crucial element of your business cyber security strategy. It ensures that, with our support, your business can respond to new threats swiftly and decisively, minimising or mitigating threats entirely.