YOUR CREDENTIALS HAVE BEEN COMPROMISED - WHAT ARE YOUR NEXT STEPS?

You've just discovered compromised employee credentials and other sensitive data of your company exposed and available on the **dark web**.

The reality is, once exposed on the dark web, your information cannot ever be completely removed or hidden. You cannot file a complaint or contact a support line to demand your data be removed.

Your company should immediately start taking appropriate steps and measures to correct or minimize the risks and potential damages associated with this exposed data. Identify, understand and learn from past mistakes or failures and adopt a more proactive and preventative cybersecurity strategy moving forward.

Remediation tips for exposed logins

□ **Replace exposed login passwords** with new, unique passwords.

□ **Change/refresh** any passwords older than six months.

□ If the source of the **breach is "not disclosed,"** change the passwords of any accounts you know you used the same or similar password for.

□ If you can't remember the passwords for all your accounts, change them all. **If you want to be safe, you'll need to update all of your passwords.** We know it's inconvenient, but it's the only way to ensure your online accounts are secure.

□ **Password awareness:** Many people use the same username and password on multiple websites. If you use the same credentials or a variation of the same password across numerous sites, ensure that the passwords are changed to make them unique.

□ **Adding $, ! or any other special characters** or numbers to a password does not make it unique.

□ **Don't use passwords that are easy to guess**, such as your pet's name, spouse's name or favorite sports team.

□ **Watch out for phishing emails.** We've seen a significant increase in phishing attacks against emails that have been discovered on the dark web.

□ We recommend **keeping an eye on any suspicious activity** on your online accounts if the reported compromise does not include a password. Check for suspicious or otherwise questionable emails on a regular basis.

□ To keep track of your passwords, **consider using a password manager**.

□ **Close unused accounts**. If a previous employee's credential was compromised, double-check if all third-party sites they had access to were turned off.

What can you do to minimize the risk of this happening again?

□ IMPLEMENT MULTIFACTOR AUTHENTICATION

Even the strongest and most complex passwords won't protect you if they have been compromised and exposed on the dark web. Requiring users to verify who they say they are via two or more unique security factors will virtually eliminate more than half the threats and risks associated with exposed user credentials.

□ CONSIDER A PASSWORD MANAGEMENT SOLUTION

A password management platform will enable your entire workforce to adapt and thrive in a security-first environment while reducing password frustration and fatigue for users and empowering increased productivity.

□ ONGOING SECURITY AWARENESS TRAINING FOR USERS

Users continue to be the weakest link in security for businesses worldwide. This is often due to genuine ignorance regarding security best practices and a lack of knowledge or awareness of common threats and risks. Establish ongoing security awareness training for all users and turn your weakest link into your most robust security defense.

□ PERFORM REGULAR RISK ASSESSMENTS

A comprehensive audit of your business infrastructure and systems will inevitably reveal vulnerabilities and security gaps within your network, applications or on your devices. Regular assessments will keep you informed and enable you to achieve and maintain a more preventative approach to security, often preventing issues or problems from arising in the first place.

□ PROACTIVELY MONITOR FOR BREACHES AND CYBERTHREATS

Cyberthreats continue to increase and evolve, and hardware and software vulnerabilities are discovered regularly, exposing your business to a steady barrage of security risks. To adopt a proactive and preventative approach to cybersecurity, your business must have visibility and insight into internal and external activities, trends and threats to your organization's network and data.

□ BACK UP EVERYTHING

You must ensure your business and customer data is protected and secured against any incident or disaster such as system failure, human error, hackers, ransomware and everything in between. In addition, make sure you explore the importance of accessibility and consider investing in business continuity as part of your backup strategies.

□ INVEST IN CYBER LIABILITY INSURANCE

Sometimes things don't work out no matter how much effort you put into them. As a business, you must do everything right. However, a hacker only needs a single gap or weak point in your security systems to slip past your defenses like a trojan horse. Every business in operation today needs cyber liability insurance to protect itself when all else fails.

Comprehensive security solutions are difficult to implement, time-consuming and may require IT expertise that your company lacks. Working with a managed service provider like us can relieve you of the hassle while also providing the peace of mind that you deserve. ***Contact us for a no-obligation consultation.***