Intellesec
CYBER SECURITY SIMPLIFIED
www.intellesec.co.uk

Your Credentials Have Been Compromised - Now What?

You've just discovered there are compromised employee credentials or 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 approach to your business' cybersecurity strategies moving forward.
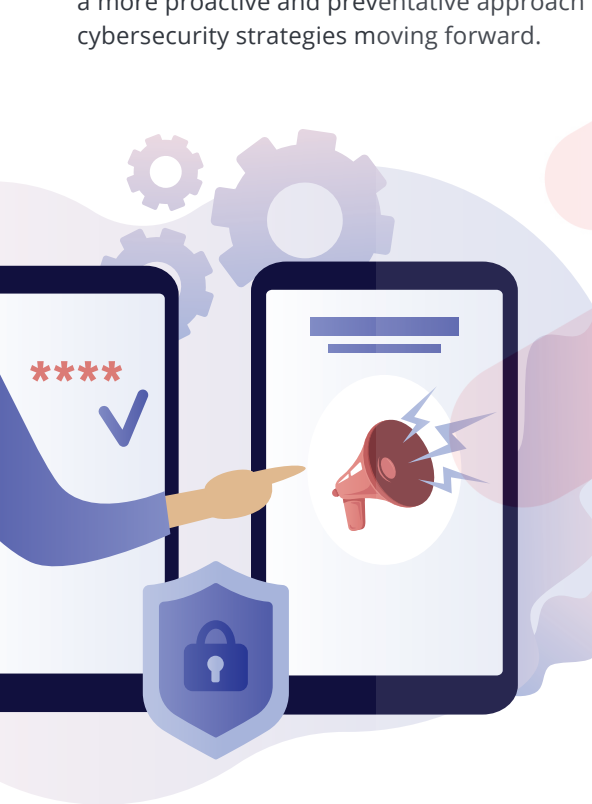
Sound the Alarms Important Business Alert

- [ ] Alert all employees, top to bottom, of the compromised data and explain or educate them about the Dark Web

- [ ] Review individual compromises with critical users
  - *Explain specific threats and risks – both to the business and potentially, the user*

- [ ] Establish/update strict password policies and review and share with users
  - *Retire old and exposed passwords*
  - *Define what a strong password is and implement a password construction policy*
  - *Make different passwords for each business account mandatory and keep personal ones separate*
  - *Determine a schedule for routine password changes*

Change Passwords

1) Change passwords for exposed logins – all accounts using the compromised passwords

   2) *Replace with unique passwords for each account*

   3) *Change/refresh any passwords older than six months*

Cybersecurity Best Practices to Proactively Protect Your Business

1) Implement Multi-Factor 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.

2) Consider Single Sign On (SSO) and Password Management Solution

The combined benefits of a Secure SSO and 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.

3) 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 strongest security defense.

4) 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. Performing regular assessments will allow you to stay in the know and enable you to achieve and maintain a more preventative approach to security, often eliminating issues or problems before they arise.

5) Proactively Monitor for Breaches and Cyber Threats

Cyber threats 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 both internal and external activities, trends and threats to the network and data.

6) Back Up Everything

It is imperative that you 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.

7) Invest in Cyber Insurance

Sometimes things do not 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 their business when all else fails.

DON'T WAIT UNTIL YOU ARE THE NEXT NEWS HEADLINE OR STATISTIC. CONTACT US TODAY TO START IMPLEMENTING THE COMPREHENSIVE SECURITY SOLUTIONS YOUR BUSINESS DESERVES.

Intellesec
CYBER SECURITY SIMPLIFIED
www.intellesec.co.uk