IPO Digital Solutions | Your Business I.T. Specialists

Why monitoring for exposed credentials is essential in protecting your organisation.

Cyber criminals are scanning the internet for poorly protected or unprotected organisations and businesses.

Usernames and credentials represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defences can easily steal hundreds or even thousands of credentials at a time.

Credentials are compromised through 4 main different types of attacks

1. Phishing – sending emails disguised as legitimate messages, tricking users into disclosing credentials, deliver malware that captures credentials.

2. Watering Holes – Targeting of a popular site, social media or corporate intranet

3. Malvertising – Injecting malware into legitimate online advertising networks and or capturing visitors credentials

4. Web Attacks – Exploitation of internet facing company assets where they are vulnerable to gain a foothold and move through the network to discover credentials

Passwords are the most common method of logging into services and are often hacked.

What can an attacker do with compromised credentials?

- Send Spam from compromised email accounts thus destroying your businesses reputation
- Deface Web Properties and host malicious content, making your website a dangerous website that will be blocked by google and others. This will cost you time and money to remedy and your website will always be on a watch list from this time forth.

- Install Malware and compromise systems

- Compromise other accounts using the same credentials

- Exfiltrate sensitive data. If your clients' data is breached, you will face fines of up to $7000 by the Australian Government and may also face litigation from your clients.

- Identity Theft

Monitoring for exposed credentials ensures that you take a proactive rather than a reactive strategic stance, it ensures you are better protected against new attacks and new forms of Phishing and the like. Privacy law and compliance are a requirement for businesses in Australia. You need to stay protected not only for your organisations security in ensuring downtime and delays in IT related assets don't occur but for the protection of you clients and their personal and organisational information.

IPO Digital Solutions

Your Business I.T. Specialists