FOCUSNET TECHNOLOGY

info@focusnet.com.au
1300 077 777
www.focusnet.com.au



# dark web STATUS REPORT

**CONFIDENTIAL**

Audit Type: Dark Web Status Review
Completed For: **XXXXXXX**

Date Completed: **8/5/2024**
Report Produced By: **David Baines** (Cyber Security Specialist)
QA By: **Luke Ide** (Sales & Marketing Executive)

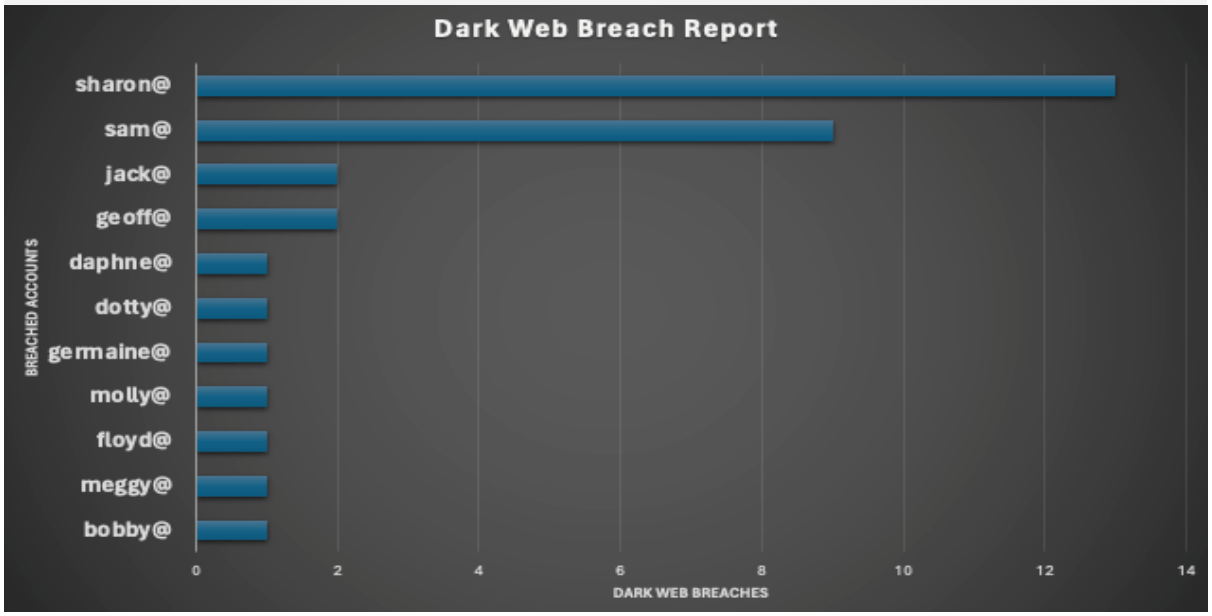
# Dark Web Status

LOW — DARK WEB EXPOSURE — HIGH

**MEDIUM TO HIGH**

## What you should know:

Dark web exposure poses significant risks. Exposed employee information can fuel convincing social engineering attacks, such as phishing and phone scams. Scammers leverage accurate details to appear trustworthy. Passwords and account data exposure can lead to unauthorised access and major breaches. Promptly inform affected employees, update passwords, and provide education to prevent future issues. Even if no breaches are found, stay vigilant as threats can arise anytime.




# You're exposed: Don't ignore this!

Many cyber-attacks begin with the acquisition of credentials previously leaked onto the dark web, and then escalate into a serious incident because businesses were either not aware of this exposure or were aware but then **chose to ignore it**.

Understanding your overall cyber status is a relatively simple process and is usually accomplished by engaging the services of a cyber security specialist.

FocusNet Technology are experts in this field and have been delivering cyber services to the SME space for years.

Whilst no-one can "un-leak" those credentials reported above, we can quickly help you understand your overall cyber risk, implement mitigations and help ensure that you don't become the next cyber victim struggling for survival.

***The internet never forgets. Once your credentials are on the dark web, it's forever!***

# How to protect your business

We know this information can be alarming and quite frankly, scary, but it doesn't have to be! We share this information with you to keep you informed so you can proactively prevent this compromised information from coming back to harm your organisation in the future. We strongly recommend that all impacted employees take the following steps towards remediation.

1. **Update your password on the compromised account.**
2. **Be wary of an increase in phishing emails being sent to you.**
3. **Avoid using your business email address for non-business activities and account management.**
4. **Change the password for all accounts where this password may have been reused and remember to use strong, unique passwords for all your accounts.**



info@focusnet.com.au 1300 077 777 www.focusnet.com.au Sydney | Melbourne | Perth

# Background

## What is the Dark Web?

The Dark Web functions as a cyber black market where stolen information is sold. Cybercriminals profit by selling previously breached data to other criminals, often without our knowledge. As their activities remain lucrative, breaches and phishing scams persist, leaving employee data and entire organisations vulnerable.

## Purpose of this Report

Cyber threats are becoming increasingly common and sophisticated in today's digital age. Personal information being sold on the dark web is one of the most significant risks that can expose individuals and organisations to vulnerabilities. To safeguard against this, knowing if employees have been involved in any dark web breaches is essential. By being aware of your organisation's dark web status, you can take proactive measures, such as securing compromised accounts and remaining vigilant for targeted phishing attempts to protect your organisation.

In today's digital age, cyber threats are on the rise, becoming more sophisticated. The sale of personal information on the dark web poses a significant risk, exposing individuals and organisations to exploitation. To help mitigate this risk, it's crucial to determine if employees have been part of any dark web breaches so you can take any actions deemed necessary.

This report will make you aware of your organisation's dark web status allowing for proactive measures, including securing compromised accounts and staying vigilant against targeted phishing attempts.

# What's the actual 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.

## Organisation Exposure

| 2 | 1 | 2 |
|---|---|---|
| Accounts scanned on the Darkweb. | Accounts exposed on the Darkweb. | Breaches your organisation has been involved in on the Darkweb. |

## 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 unauthorised access to your network where they can wreak havoc.

Someone at your organisation had data exposed on the dark web... what happens now? Unfortunately, the impact of a third-party data breach involving your or one of your employee's business accounts could be a vulnerability to your business. Read on to learn what you can do to proactively address these hidden threats.

# Who is FocusNet?

This report was produced by FocusNet at the request of your Insurance Broker because we both care about your cyber risk profile and true cyber exposure.

Statistics tells us that, in Australia, 60% of Small/Medium businesses that experience a significant Cyber incident do not survive and ultimately go out of business within 12 months of the incident.

FocusNet are data security experts and provide a cohesive range of data and cyber services to the SME space that are informative, effective and affordable for everyone. Our team prides itself on the ability to strike the balance between robust security and powerful performance. With a consultative approach to your business, our friendly consultants are well equipped to listen, identify issues, and set out a comprehensive roadmap of recommendations to fulfil your unique requirements.

Below are some of the key business services available in FocusNet's Cyber suite:

## E8 Cyber Health Checks

Comprehensive Cyber review of your business based on the ACSC Essential Eight maturity model and NIST standards. Includes detailed findings and recommended mitigations.

## Cyber Advisory & Risk Mitigation

Expert Cyber advisory is a critical support service for every modern-day business - Cyber incident prevention, cyber risk management, cyber incident response.

## Penetration Testing

Internal stress testing of your IT environment to expose any cyber risks and recommend strategies to be implemented to reinforce your cyber posture.

## Staff Security Awareness Training

A training platform designed to reduce staff's risky online behavior via Phishing simulations, training content, cyber policy management and effective reporting.

# The Next Step

Whilst finding user credentials on the Dark Web might not be the end of the world, it definitely is a big red flag and shouldn't be ignored.

In light of discovering these leaked credentials, concerned businesses generally seek to understand their cyber risks more deeply by consulting with a cyber security specialist. Gaining this insight allows them to address vulnerabilities and stay ahead of potential threats.

While you may already have an IT service provider, an independent review provides an objective perspective on your cyber resilience. Our E8+ Cyber Health Check offers an unbiased evaluation that can complement your existing IT support, helping you to ensure that all bases are covered.

To explore how we can help improve your business's cyber posture, please contact our Cyber Security Specialist for further advice and information.

**Dave Baines**
Msc. Cyber Security, OSCP, OSEP
Cyber Security Specialist
david.baines@focusnet.com.au
(08) 6500 0505