Dark Web Sample Report

DARK WEB FACTS

The dark web is a massive and widely used marketplace by cyber criminals

Malicious actors use stolen email credentials to impersonate the owner to commit theft or other fraud

The stolen records including identity and credit card information are often sold on the dark web

RISKS DETECTED FOR YOU

04 **Unique Email IDs Found**
Some email IDs may have multiple breaches

Email ID	Password	Publish Date	Breach Source
user1@test.com.au	Encrypted	Jan 11, 2020	Not Disclosed
user1@test.com.au	Encrypted	Jan 27, 2020	imesh.com
user1@test.com.au	Encrypted	Feb 17, 2020	Not Disclosed
user1@test.com.au	bel*****	Feb 19, 2020	Not Disclosed
user2@test.com.au	Encrypted	Feb 21, 2020	Not Disclosed
user2@test.com.au	280*****	Mar 1, 2020	animoto.com
user3@test.com.au	280*****	Mar 10, 2020	Not Disclosed
user3@test.com.au	Encrypted	Mar 12, 2020	Not Disclosed
user3@test.com.au	280*****	Mar 14, 2020	myspace.com
user4@test.com.au	280*****	Mar 17, 2020	Not Disclosed
user4@test.com.au	Encrypted	Mar 18, 2020	animoto.com

HOW TO GET PROTECTED?

- *Follow best security practices*
- *Your identity safe by keeping passwords Complex*
- *We scan Dark web & take actions*

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

STAY SECURED.

Dark Web Sample Report

DARK WEB FACTS

Forged email is when it appears to be genuine but is sent from an untrust worthy source

Unreliable sources send more than 150 million fraud emails daily

Of those emails, 16 million make it past email filters, and thousands are clicked

RISKS DETECTED ON YOUR EMAIL SERVERS OR DOMAINS

01 Risks Detected On your Email Servers Or Domains

LIST OF YOUR EMAIL DOMAINS	SPF*	DMARC**
@test.com.au	✓	✗

Complete anti-spam configurations require the configuration of DKIM. DKIM uses keys to make sure an email sender is who they say they are. Email domains can contain multiple DKIM cryptopraphic keys. If you are unsure that your domain has DKIM enabled contact your email administrator for assistance.

Remediation

Configuring SPF, DKIM and DMARC for your domains makes it significantly more difficult for a malicious actor to send emails impersonating your organization.

***SPF** or Sender Policy Framework, is an open standard that specifies a method for preventing sender address forgery. It isn't about stopping spam; it's about controlling and stopping attempted sender forgeries.

****DMARC** or Domain-based Message Authentication, Reporting, and Conformance, enables the message sender to indicate that their message receiver to follow if an email does not pass SPF or DKIM authentication.