Prepared by:
One2Call

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 stolen on dark web

RISKS DETECTED FOR YOU

09 **UNIQUE EMAIL IDs FOUND**

Some email IDs may have multiple breaches

Email ID	Password	Publish date	Breach Source
allen@company.com	A1c*******	Jun 25, 2020	Not Disclosed
allen@company.com	A1c*******	Feb 06, 2019	Not Disclosed
allen@company.com	A1c*******	Jan 29, 2019	Not Disclosed
allen@company.com	A1c*******	Dec 20, 2018	Not Disclosed
allen@company.com	A1c*******	Jul 28, 2018	Not Disclosed
bailey@company.com	Encrypted	Oct 24, 2016	dropbox.com
bailey@company.com	Encrypted	Oct 21, 2016	adobe.com
caroline@company.com	fra*******	Feb 06, 2019	Not Disclosed
caroline@company.com	fra*******	Feb 06, 2019	Not Disclosed
caroline@company.com	fra*******	Jan 29, 2019	Not Disclosed
caroline@company.com	fra*******	Jan 29, 2019	Not Disclosed
caroline@company.com	fra*******	Dec 22, 2017	Not Disclosed
caroline@company.com	fra*******	Oct 18, 2017	Not Disclosed
caroline@company.com	fra*******	Oct 09, 2017	Not Disclosed
caroline@company.com	Encrypted	Oct 21, 2016	linkedin.com
danni@company.com	3&r*******	Feb 06, 2019	Not Disclosed
danni@company.com	3&r*******	Jan 29, 2019	Not Disclosed
danni@company.com	Encrypted	Oct 24, 2016	dropbox.com
finance@company.com	71o*******	Jan 16, 2018	facebook.com
nile@company.com	Encrypted	Oct 24, 2016	dropbox.com
nick@company.com	Encrypted	Oct 24, 2016	dropbox.com

RISKS DETECTED FOR YOU

Email ID	Password	Publish date	Breach Source
pete@company.com	Encrypted	Oct 24, 2016	dropbox.com
support@company.com	Encrypted	Oct 24, 2016	dropbox.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 acounts 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.

Prepared by:
One2Call

SENDER EMAIL FORGERY AND SPAMMING

Forged email is when it appears to be genuine but is sent from an untrustworthy 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 DOMAINS HAVE INCOMPLETE ANTI-SPAM CONFIGURATIONS

List of your email domains	SPF*	DMARC**
@company.com	✓	✗

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 cryptographic 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 messages are protected with SPF and/or DKIM. A DMARC policy applies clear instructions for the message receiver to follow if an email does not pass SPF or DKIM authentication.