NETWORK BOX

NEXT
GENERATION
MANAGED SECURITY

The Dark Web:
the dark side of the Internet

Jan Van Leersum
Network Box Singapore
Managing Director

www.network-box.com

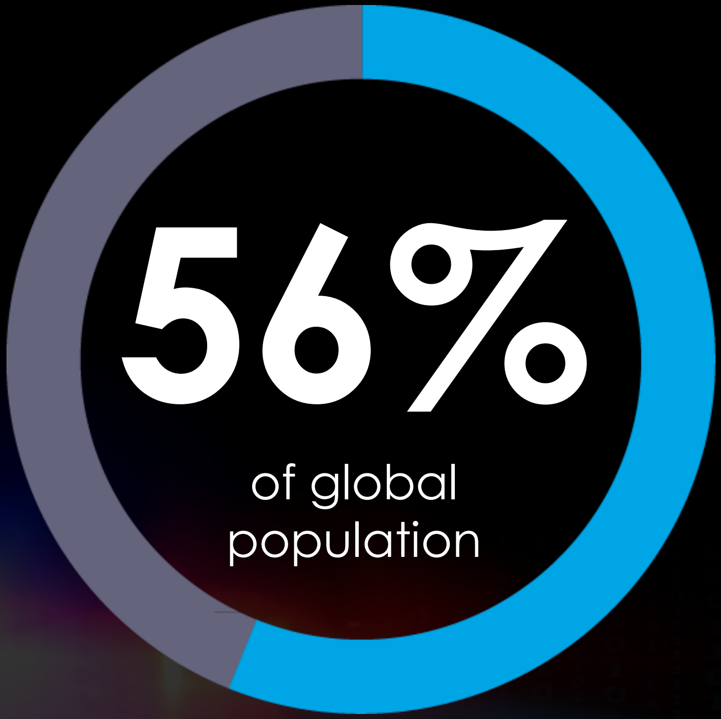
The Internet has become an essential part of our daily lives

NETWORK BOX

There are over

4.3 billion

Internet users across the world.



Source: https://www.statista.com/statistics/617136/digital-population-worldwide/

NETWORK BOX

Governments and organizations have either forced or enticed, almost everyone to handover unimaginable quantities of personal data.

For registration and access, users freely give them all their personal data:

- Full names
- Birthdates
- Phone numbers
- Physical addresses
- Bank account details
- Credit card numbers
- Passport numbers
- Medical records
- Travel itineraries
- Personal photos and videos
- Children's information

All this information is then aggregated, and stored in massive databases.

However, these databases are not being properly secured.

117 million

LinkedIn user's login credentials were stolen.

Source: http://www.bbc.com/news/technology-36320322

500 million

hotel guest details hacked

- Name
- Home address
- Phone number
- email address
- Passport number
- Date of birth
- Arrival and departure information

Source: https://www.newsweek.com/marriott-hack-massive-data-leak-hits-500-million-customers-hotel-breached-1238449?fbclid=IwAR33RW3n1Bcp-U0eA94ibxmaimeb5X1DbccFTQs7goQsa1JJam_NydUVwuo

3 billion

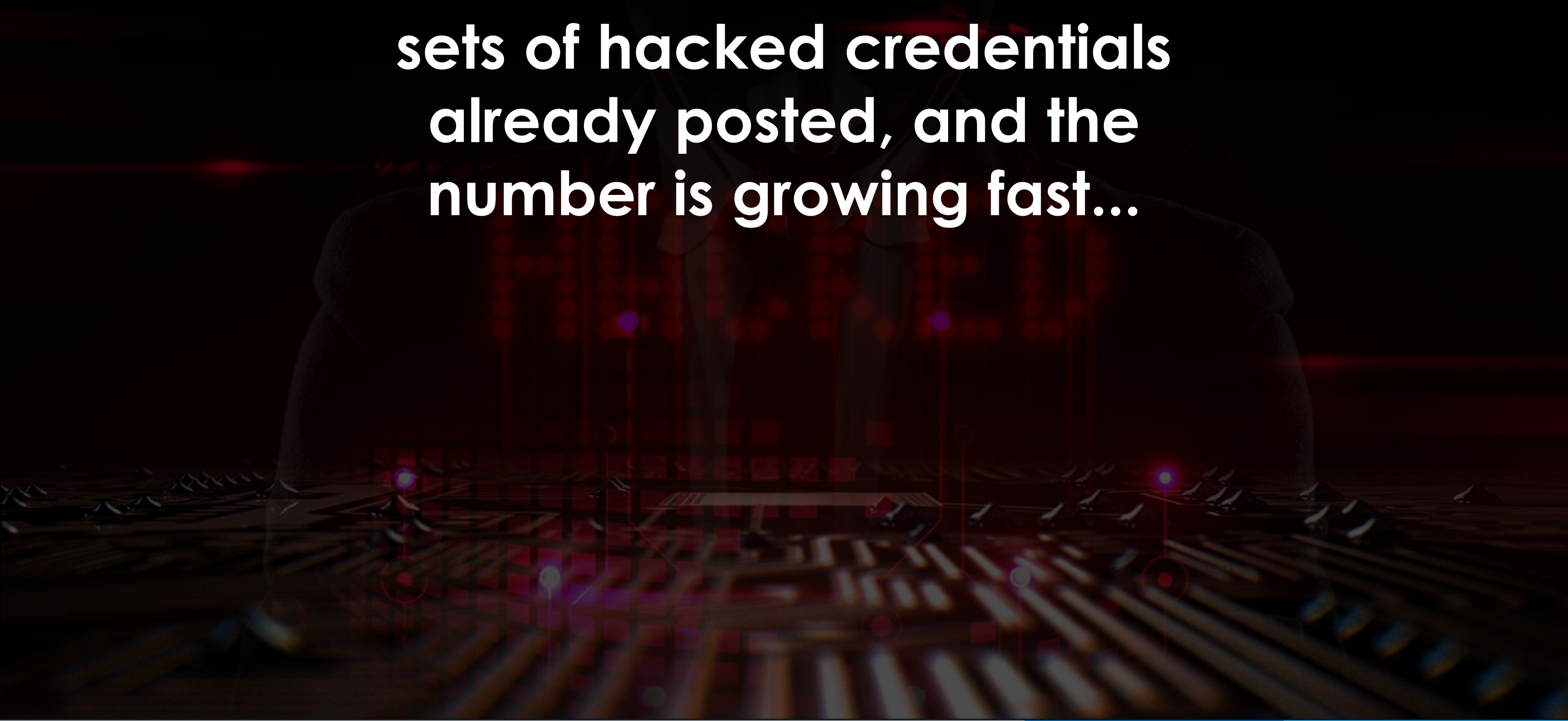
Yahoo! user accounts were hacked containing personal information.

Source: https://www.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/

Whenever there is a massive data breach, that stolen personal data usually ends up on the Dark Web

NETWORK BOX

There are currently over 6.5 billion sets of hacked credentials already posted, and the number is growing fast...

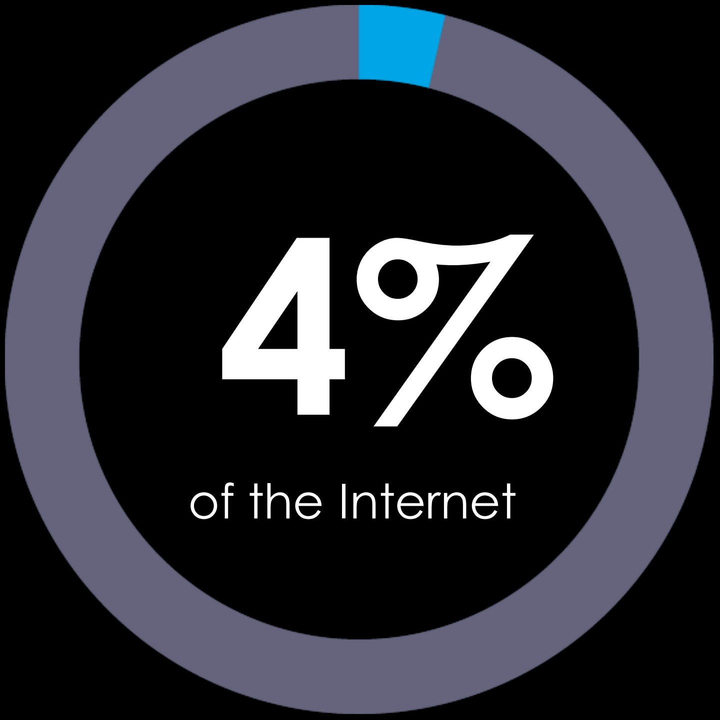


Source: https://www.independent.co.uk/life-style/gadgets-and-tech/news/collection-1-data-breach-latest-more-information-cyber-security-a8734736.html?fbclid=IwAR21fzIvW23RpjkAXApz_B1H2J5eZv3KOyMvNo507hJu7kBxbU37HQ_R4KY

What is the Dark Web?

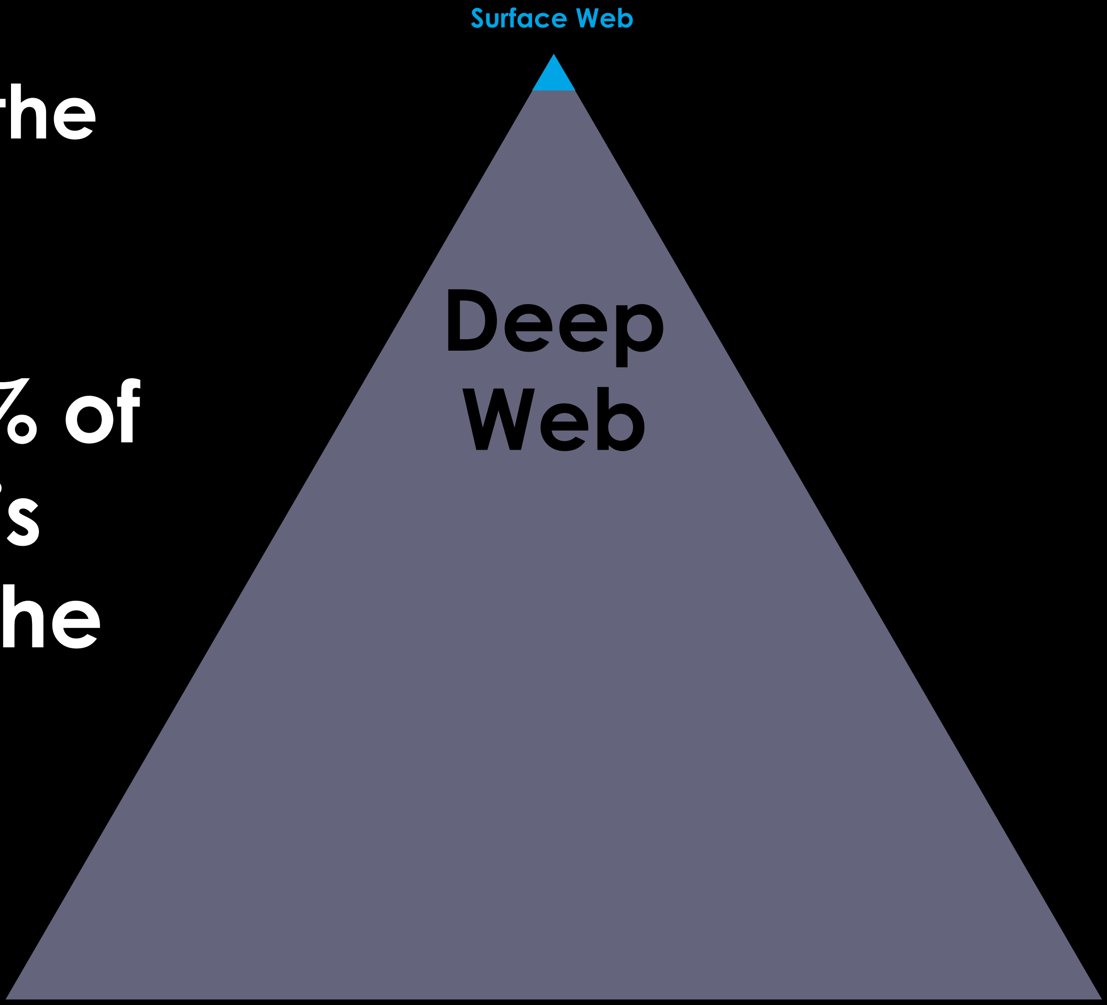
Only 4% of the Internet is publicly accessible, and indexed by normal search engines such as:

- Google
- Yahoo
- Bing



This is known as the
Surface Web

The other 96% of the Internet, is made up of the Deep Web

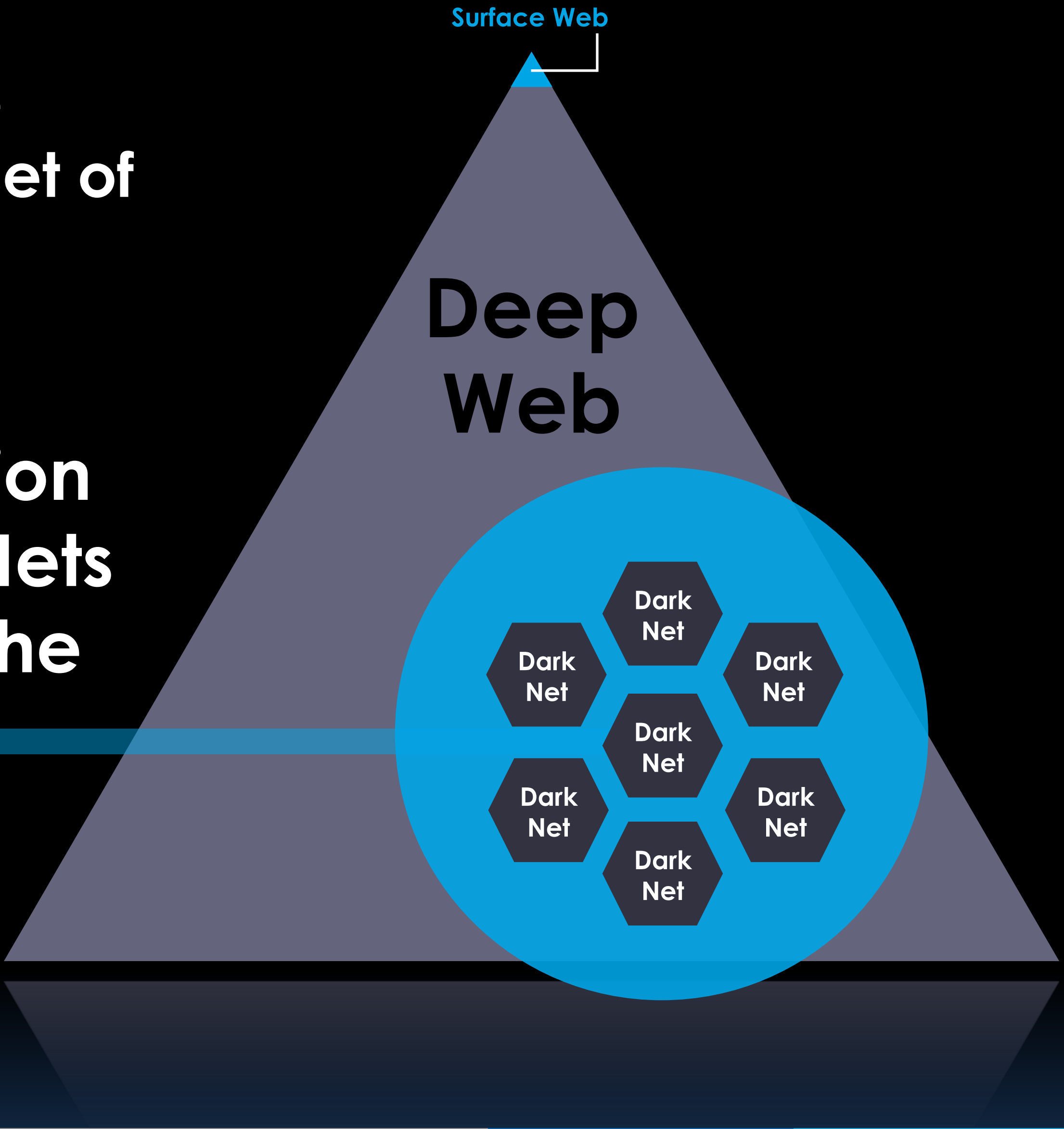


The vast majority of people, companies, and organisations, use the Deep Web to store confidential information:

- Company accounts
- Product designs
- Customer data

However, within the Deep Web is a subset of Dark Nets

It is the collection of these Dark Nets that make up the Dark Web



The Dark Web is the deliberately hidden part of the Internet, which cannot be accessed without specialist knowledge, and specific software tools.

Different tools, are used to access different Dark Nets:

- **T.O.R**
  (The Onion Router)
- **Riffle**
- **Freenet**
- **I2P**
  (Invisible Internet Project)

Not everything that happens on the Dark Web is criminal:

T.O.R (The Onion Router) was developed by the United States Naval Research Laboratory, to help protect U.S. intelligence traffic being sent over the public internet.

Political dissidents often communicate to each other using the Dark Web to remain anonymous, and protect themselves.

NETWORK BOX

However, if something criminal is happening online, it is probably happening on the Dark Web

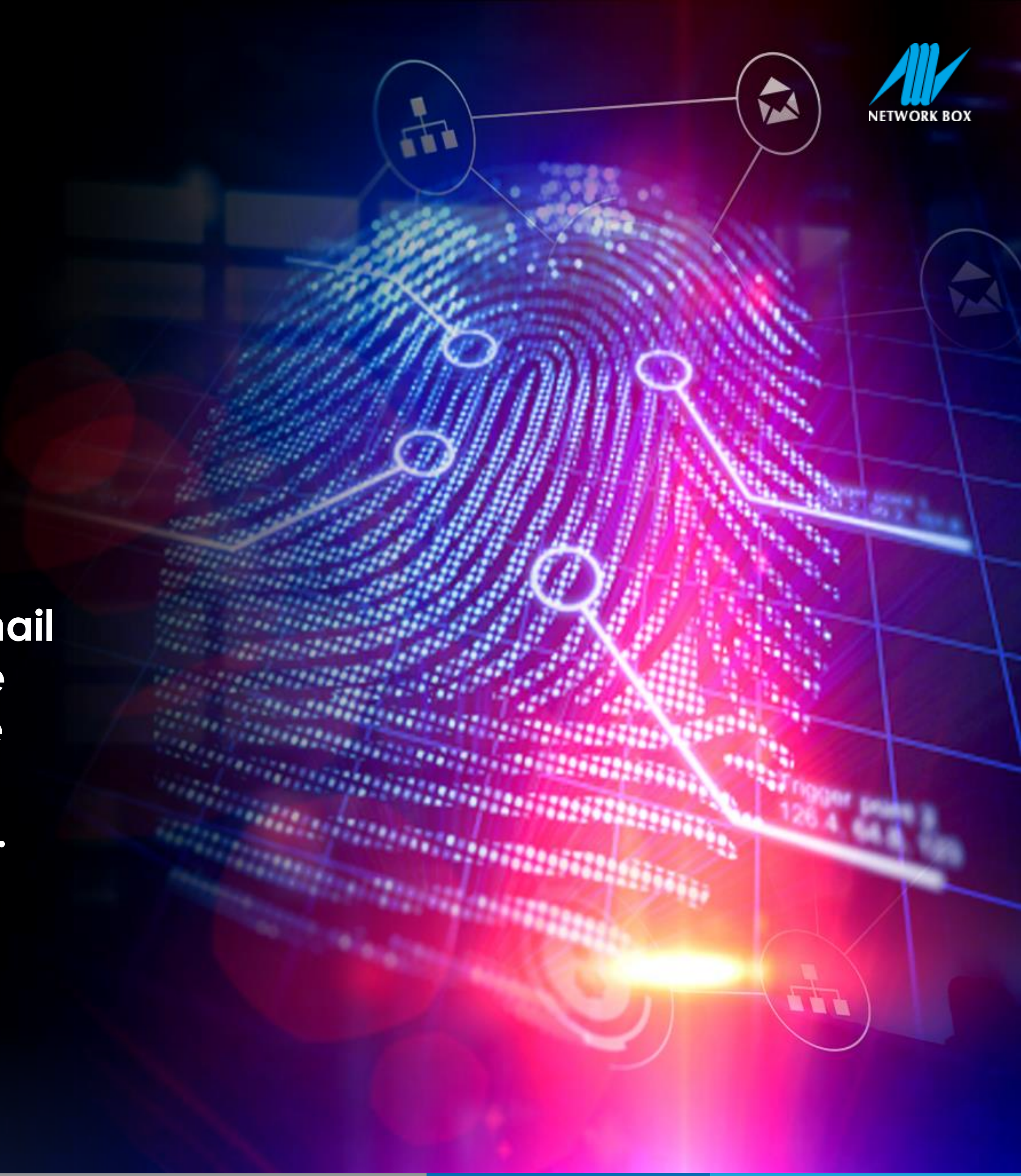
How this impacts YOU

Loss of privacy, your information is available to everyone

If a third-party site you are using gets hacked, your personal data may become available to everyone on the Dark Web, forever.

Your email address is your unique digital fingerprint

If a hacker gets your email account details from the Dark Web, you could be pwned, and tracked across different services.



Hackers can use your information for identity theft

By using your data found on the Dark Web, hackers may know more about you than you do.

Direct access to your company network, and critical accounts

If a hacker wants to gain access to your account or company network, he could perform a Dark Web search for your credentials.

You could be targeted for blackmail hoaxes

Hackers are sending out millions of phishing emails, claiming that they have hacked victims' servers, web-cams, and even their physical offices.

What to do if your details are found on the Dark Web

NETWORK BOX

Force a password reset on your internal systems

Usernames and passwords found on the Dark Web could be used to infiltrate your company network and internal systems.

Implement a company-wide Password Policy

- Change your password at least once a quarter.
- Use a strong password:
  - 12-15 characters
  - Capitalize two or more characters
  - Use numbers and special characters
  - Don’t use birthdays or phone numbers
- Enable Multi-Factor Authentication with a Time-based One-Time Password (TOTP).

Separate your work from your personal on-line activities

DO NOT to use your work email address for non-work related websites.

It is estimated that about 30% of people, reuse passwords on multiple sites.

Educate your users about phishing emails and general Internet safety

This should not just be for general staff, but also include high level management and the Board of Directors.

Consider subscribing to a Dark Web monitoring service

There are already BILLIONS of sets of hacked credentials posted on the Dark Web, and millions more are being added all the time.

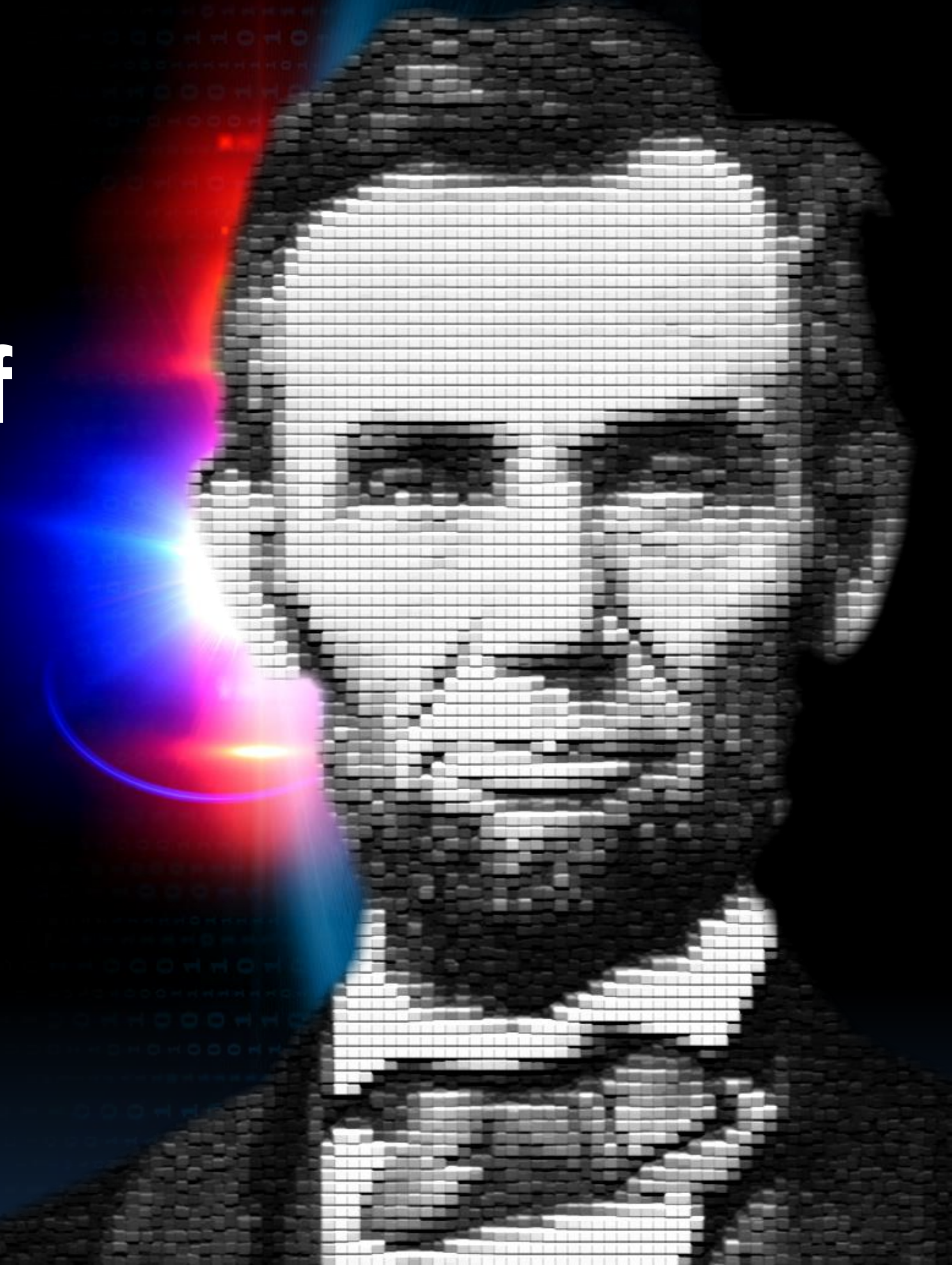
A Dark Web monitoring service provider should:

- Regularly scan the Dark Web for postings of your registered domains and email addresses
- Produce detailed reports of data breaches including compromised users, and origins of breaches
- Provide on-going monitoring, and notification of any discoveries found on the Dark Web

NETWORK BOX

You cannot escape the responsibility of tomorrow **by evading it today.**

— Abraham Lincoln



NETWORK BOX

NEXT
GENERATION
MANAGED SECURITY

Thank You and stay safe

Jan Van Leersum
Network Box Singapore
Managing Director