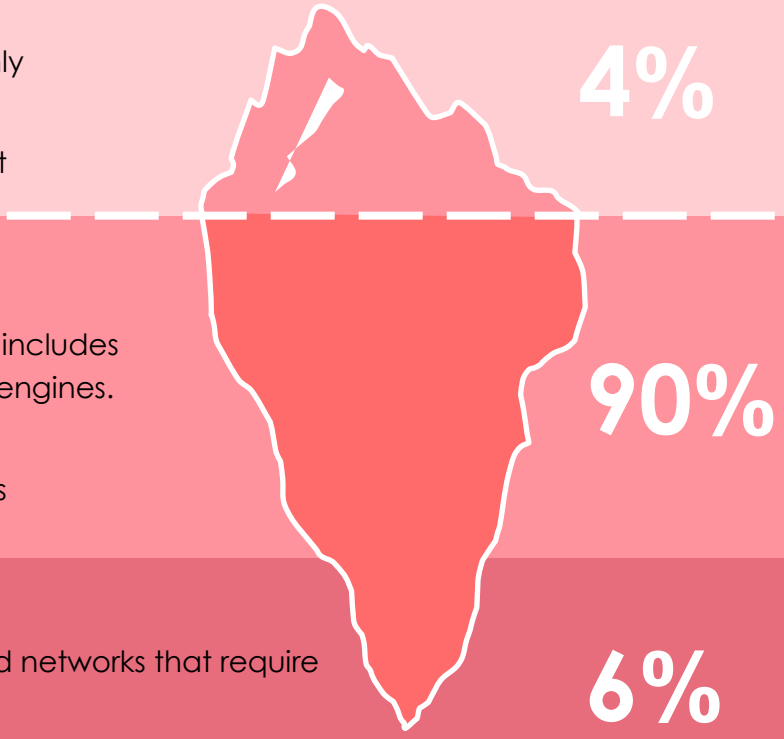
DARK WEB MONITORING

ACE Technology Group

WORLD WIDE WEB

Includes public websites which make up only 4% of Internet content.

Example: Google, Yahoo, Wikipedia, Reddit



DEEP WEB

Making up 90% of the Internet content, this includes information not accessible through search engines.

Example: Cloud Storage, Legal & Financial Documents, Patient Data, Research Articles

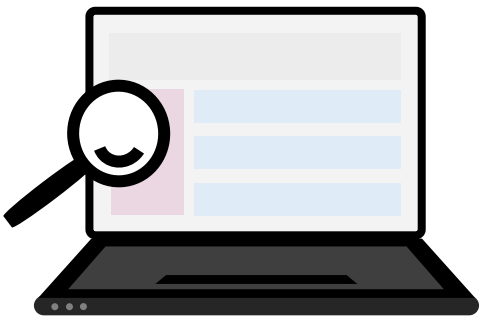
DARK WEB

About 6% of the Internet includes encrypted networks that require special software to access.

Example: Stolen Information, Illegal Websites, Hidden Marketplaces

WHY IS THIS IMPORTANT?

Dark web scans search for the presence of an organization's email domain on the dark web. Being aware of company accounts with data breaches and compromised passwords allows for companies and individuals to take action in becoming more secure and preventing a cyber attack. Compromised data will vary depending on the type of data breach it was acquired from.



DARK WEB MONITORING

Dark Web Monitoring will constantly be searching the Dark Web for compromised credentials associated with your company. If a compromised credential is found, you will be immediately alerted so that you can quickly change the compromised password on any of your accounts that are using it.

DARK WEB SCAN RESULTS INCLUDE:

Compromised Data

Compromised data signifies what data has been found on the Dark Web. The type of data can include name, address, email, etc. and can be used to craft sophisticated phishing scams.

Data Breach Details

If there are known details of the data breach an employee has been involved in, they will appear in the Data Breach Details section of the report.

Breach Score

Each breach that a domain is found to be involved in will have a breach score associated with it. This score indicates if the data leak is from a credible source.

Passwords

If a password is found on the Dark Web, those details may be available.