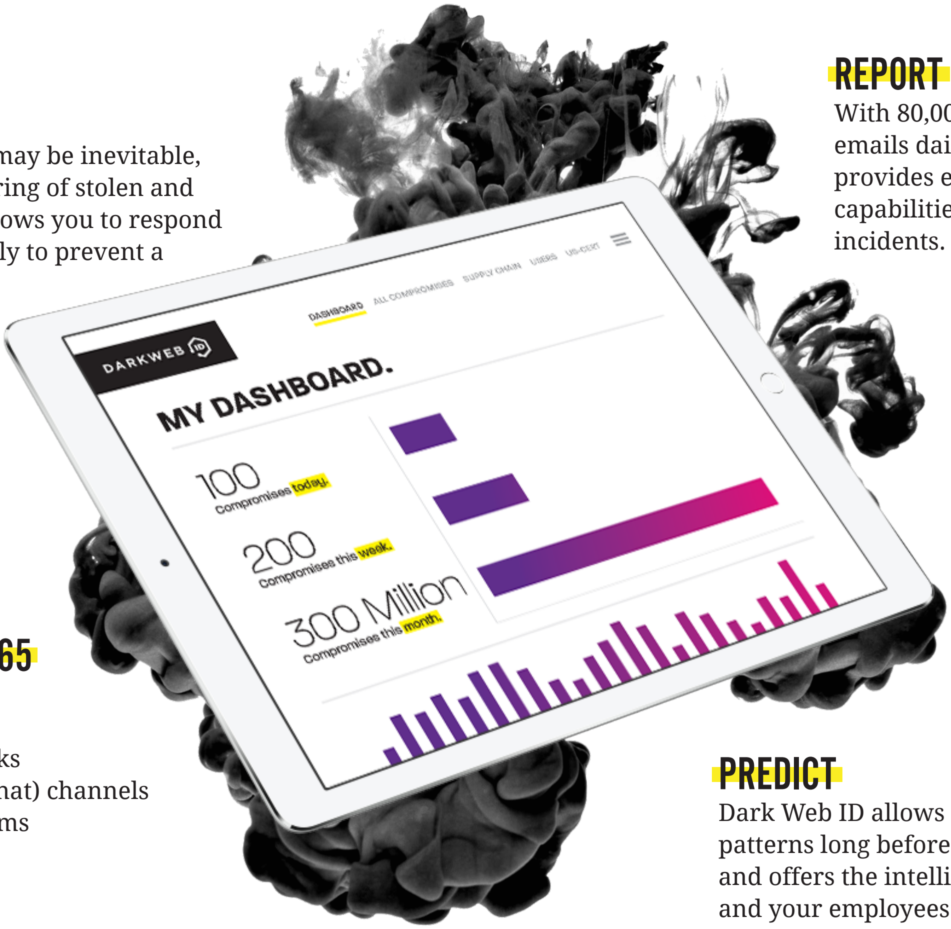
WE GO INTO THE DARK WEB TO KEEP YOU OUT OF IT.

PREVENT

Attacks on networks may be inevitable, but proactive monitoring of stolen and compromised data allows you to respond to a threat immediately to prevent a major breach.

REPORT

With 80,000+ compromised emails daily, the platform provides extensive reporting capabilities to track and triage incidents.



MONITOR 24/7/365

- Hidden chat rooms
- Private websites
- Peer-to-peer networks
- IRC (internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

PREDICT

Dark Web ID allows us to see industry patterns long before they become trends, and offers the intelligence to keep you and your employees more protected.

HOW DARK WEB ID PROTECTS YOUR BUSINESS

- Connects to multiple Dark Web services including Tor, I2P and Freenet, to search for compromised credentials, without requiring you to connect to these high-risk services directly.
- Provides intelligent awareness of compromised credentials before breaches occur.

WHY IT'S IMPORTANT

- Compromised credentials are used to conduct further criminal activity.
- Employees often use the same password for multiple services, such as network login, social media, and SaaS business applications, exponentially increasing the potential damage from a single compromised credential.
- Limited visibility when credentials are stolen; over 75% of compromised credentials are reported to the victim's organization by a third party, such as law enforcement.

FREEDOMTECH

800-940-0040 | Sales@ftssupport.com

Contact Us Today for a Free Preliminary Dark Web Scan!

DARKWEB ID

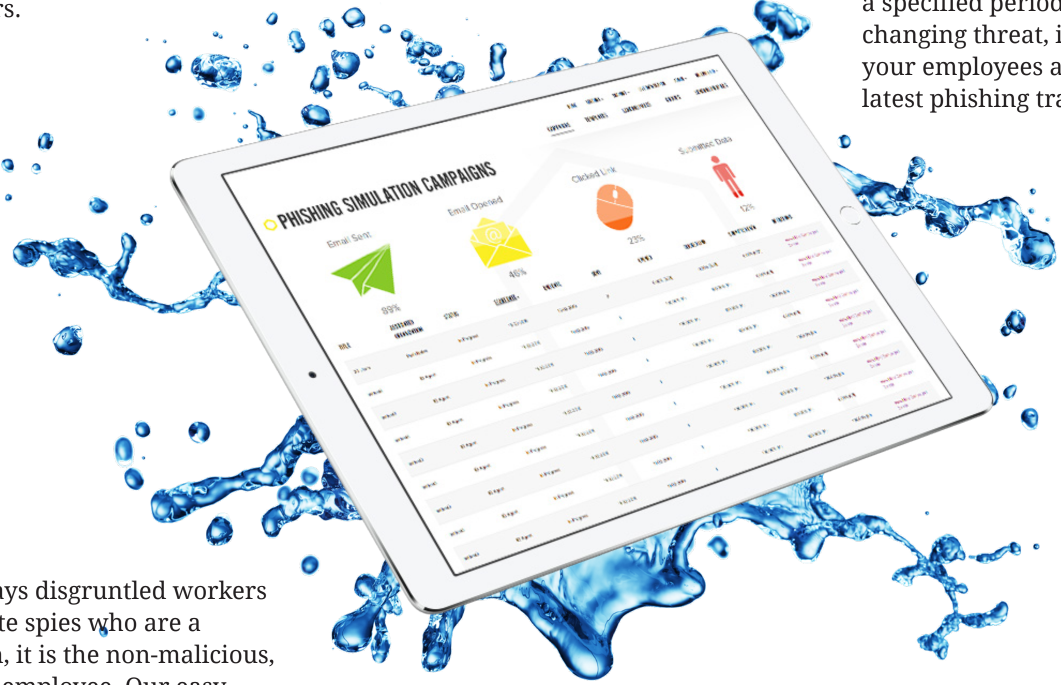
PHISHING SIMULATION & SECURITY AWARENESS TRAINING.

DETECT

Employees often use the same password for multiple services on the web, such as CRM, e-commerce sites, and social media. Proactive monitoring for stolen and compromised employee data on the dark web allows us to detect when a problem arises, before a major breach occurs.

PHISH

We can send scheduled phishing campaigns, including customized messages to fit each group or department, at random times during a specified period. With an ever-changing threat, it is important that your employees are exposed to all the latest phishing traps set by criminals.



TRAIN

It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee. Our easy-to-understand, short and visually engaging training videos end with an online quiz to verify the employee's retention of the training content.

MEASURE AND TRACK

Your regular Security Threat Report will demonstrate the overall cybersecurity posture of your organization, to include dark web credential compromises combined with employee phishing and training campaign results.

WHY YOU NEED AN INTEGRATED, ONGOING PROGRAM

- Cyber-attacks are on the rise; particularly among small- and mid-sized businesses.
- You may have the most up-to-date and strongest security systems in place, but this will be a wasted investment if you don't also train and test your staff.
- Threats are ever-evolving and become more sophisticated and harder to detect. Regular training on the latest criminal tactics will help mitigate risk.

Your employees are your first and primary line of defense against online crime. Equip them with the knowledge and skills they need to protect themselves - and your business - from criminal elements.

FREEDOMTECH

800-940-0040 | Sales@ftssupport.com

Contact Us Today for a Free Preliminary Dark Web Scan!