JK
TECHNOLOGY SOLUTIONS
SINCE 2004

DARK WEB MONITORING

Our 24/7 Dark Web Monitoring solution provides critical alerts for business domain and employee credentials. The earlier you know about these compromises, the sooner you can reset passwords and resolve these security gaps.

Why It Matters:

The presence of compromised account credentials represents a huge risk to the operations of your business. The longer a credential remains compromised, the higher the chance that sensitive information has been leaked to a threat.

Protect your business from the increased security threats caused by exposed login and password details on the Dark Web.

We leverage the power of both advanced technology intelligence and human analysts to proactively search for and analyze compromises and exposed login credentials that can make your business a hot target for cybercriminals.

24 x 7 x 365 Monitoring
- Identify and investigate exposed login credentials or pairs discovered directly linked to your business email domains or IP address details.

Overcome Password Reuse
- Individuals often reuse the same login credentials accross multiple platforms, which makes them more vulnerable to credential theft. Overcome the risks related to bad passwords.

Alerts and Report Analytics
- With 80,000+ domain compromises discovered daily, access reporting and analytics on industry trends and evolving risks and take preventative actions to avoid cyber threats.

Proactive Prevention
- Cyberattacks are becoming increasingly inevitable. However, implementing Dark Web monitoring will help reduce the risks and threats caused by exposed employee credentials.

LET US HELP YOU CONQUER YOUR CYBERSECURITY CHALLENGES. CONTACT US TO LEARN MORE.

866-634-9633

jkconsulting.com

Your Learning Management Platform for Security & More

Get an engaging training platform that instills a security-focused culture and equips your organization to create its own training courses and upload/deploy them to relevant team members.

Your Business Risks

Your weakest link against security threats?
Your employees.

The average cost of a data breach is $4.24 million.[1]

A learning management solution serves as a foundation on which to train and educate your employees on security best practices. This can greatly decrease the likelihood of a breach.

Our training platform consists of built-in phishing training and comes with the option of letting your organization create its own training courses and upload/deploy them internally. This can include, but is not limited to, employee safety, conduct (anti-harassment) and more. It could even be used for human resources (HR) training such as employee onboarding, policy training, etc.

Why Training Is Essential

85% of breaches involved the human element in 2020.
36% of breaches involved phishing in 2020, up 11% from
last year.[2]
61% of data breaches included credential theft in 2020.[2]

Sources:
1 Ponemon 2021 Cost of a Data Breach Report
2 Verizon 2021 Data Breach Investigations Report

SIMULATED PHISHING
Test simulations that mimic real-life phishing and business email compromise attacks can be launched as often as desired and automatically staggered to prevent employees from receiving the emails all at the same time.

ENGAGING TRAINING
Your workers are more likely to grasp and adhere to training if it is engaging and informative. Short, animated explainer videos and quizzes provide an efficient and measurable learning environment.

CUSTOMIZABLE SCHEDULES
Keep employee skills up to date and make security awareness a routine by customizing your training schedule. Launch on-demand training or set it to launch regularly on a weekly, bi-weekly or monthly basis.

ANALYTICS & REPORTS
Robust analytics track and measure the effectiveness of your campaign, reporting results for the whole workforce right down to individual
team members needing additional