

CyberProtectSM : Digital Risk Protection

Targeted Solutions for Proactive Detection
and Removal of Emerging Threats Across the
Internet and the Dark Web

Cybercriminals use phishing, social media sites, steal credit and debit cards, and harvest personal information and credentials to deceive your customers and take over account data. This solution helps you stay ahead of them.

With CyberProtect: Digital Risk Protection from Fiserv, you can deploy targeted threat intelligence resources to meet your organization's specific needs:

- Detect deception tactics, such as the creation of lookalike domain names and webpages used to victimize your clients; this capability includes a takedown service for malicious domains
- Identify freshly stolen credit cards and highlight usernames and passwords compromised in the underground economy, to help prevent account takeover attacks
- Discover fake social media accounts that resemble or utilize a your name and/or graphics, including Facebook, Twitter, Instagram, and LinkedIn
- Detect rogue applications that resemble and/or utilize your name and/or graphics in 170+ unofficial app stores



Protect the Brand You've Worked So Hard to Build

Successful phishing attacks negatively impact your customers and your organization's reputation, and often result in revenue loss. Attackers use a variety of methods to steal information, from setting up fake websites, to using malicious email campaigns and impersonating your organization on social media. Digital Risk Protection proactively detects and disrupts the phishing attacks, app impersonations and fake social media sites targeting your customers and partners., helping to keep your reputation in tact.



Thorough Data Collection

Digital Risk Protection analyzes more than 100 million potential phishing domains daily, using a wide range of open and proprietary data sources. This process includes searching active and passive DNS records, scanning domain registration data and using advanced web-crawling capabilities.



High Fidelity Alerts

This solution combines machine learning with cybersecurity expertise to uncover websites impersonating your brand. We continuously adjust detection parameters as the threat landscape evolves.



Effective Takedown Process

Digital Risk Protection expedites takedowns for malicious domains, shortens remediation time, and automatically generates supporting evidence and reporting.



Key Features

- Detection of brand-impersonating domains, fake social media sites and unauthorized mobile applications using a wide range of open proprietary data sources
- Monitoring of new domain registrations to quickly identify phishing campaigns
- Advanced detection of lookalike domains and subdomains
- Detection of domains involved in large-scale phishing email campaigns
- Ongoing monitoring of suspicious domains and real-time alerts when phishing campaigns go live
- Takedown service that leverages our 24/7 security operation centers (SOC) to take immediate action on your behalf and quickly remove threats
- Near real-time alerts and client-facing web portal for superior reporting

Deploy a 24/7 Watch for Attempted Fraud Against Your Organization

Cybercriminals have created their own underground economy. They have shifted their communications to popular instant-messaging applications to exchange stolen account information and credentials while evading authorities. Leveraging unique access to the messaging underground, Digital Risk Protection works for you to combat these hidden threats.

Digital Risk Protection is deployed by our team of expert cybersecurity analysts. These elite, field-seasoned professionals leverage their knowledge of the deep and dark web, as well as their extensive understanding of threat actor behaviors and languages, to role-play and gain cybercriminals' trust. Our experts have learned to think, talk and act like the attackers, engaging threat actors in investigative conversations that reveal fraudulent activities and attacker trends.

Cybercriminals are hunting for usernames, email addresses and passwords, using what they find to breach your defenses. Digital Risk Protection limits your exposure to these attacks and minimizes the potential for a breach. Our SOCs around the world keep us on top of established and emerging threat actors and the well-financed tools they are developing to outsmart traditional security measures.




Key Benefits

- Constantly searches for mentions of bank identification numbers and compromised email credentials, in instant messaging as well as the deep web and dark web
- Issues alerts identifying threat actors and the platforms where they are operating
- Produces actionable and tailored intelligence through our strategic and operational external threat hunting, based on the latest threat trends in the financial sector and specific business needs
- Monitors closed groups in four distinct instant-messaging applications
- Provides continuous, 24/7 defense against emerging threats through SOCs located around the world

Connect With Us

For more information about
CyberProtect: Digital Risk Protection

 800-872-7882

 getsolutions@fiserv.com

 fiserv.com

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit [fiserv.com](https://www.fiserv.com) to learn more.