PHISHLABS

Digital Risk Protection

Detecting Risks Across Email, Domain, Social Media, Mobile, Dark, Deep, and the Open Web

Digital Risk Protection For Your Enterprise, Brands, Executives, and Customers

The digital presence of today's enterprises extend far beyond the network perimeter. The modern enterprise digital footprint spans across social media, mobile, cloud, the web, and other platforms where it is exposed a broad range of digital risks such as impersonation, exposure of sensitive data, and cyber threats.

These digital risks can cause substantial harm to the enterprise, its brands, its executives, and its customers. However, protecting against these risks is a challenge. They exist on platforms outside of the enterprise's control, where they can easily go undetected and unmitigated.

PhishLabs' Digital Risk Protection is a comprehensive service that provides proactive detection and rapid mitigation of digital risks. We continuously monitor for digital risks across email, domain, social media, mobile, dark, deep, and open web vectors.

Risks are analyzed by our two 24/7 security operations centers and then taken down. With more than 15 years of experience taking down digital risks, we have the trusted relationships and fast lanes needed to quickly deliver effective mitigation.

Ensure Exceptional Digital Risk Protection

PhishLabs doesn't offer tools, we provide solutions. As your trusted partner, we offer more than a set of tools, but also expert analysts and the resources needed to properly detect, assess, and mitigate digital risk. Our managed services include the alignment of our team alongside yours, ensuring that your security goals and objectives are met just as any of your team members would.

Rapidly Mitigate Digital Risks

When digital risks are detected, they need to be mitigated. In most cases, that means engaging with external third parties that have control over the platforms the risks live on. This can be a tedious, lengthy process. Hosting providers, registrars, social media networks, app stores, and other third parties each have their own policies and procedures for taking down content, profiles, and accounts. Given the volume of abuse on many platforms, it can take days or weeks for a digital risk to be removed.

PhishLabs' Digital Risk Protection service focuses on eliminating malicious threats to your enterprise, brands, and customers. By partnering with PhishLabs, our experts shut down reported or detected malicious or unauthorized content. When malicious content is reported or identified, our team of experts will take the necessary steps to get the threat offline. Because threats are housed and delivered in numerous ways, we use just as many tactics to bring each threat down.

PhishLabs also brings a human element to the typical automated takedown process. Over the past 15 years, we have developed strong relationships with a number of hosting providers and social platforms, which means that when they receive a request from PhishLabs it is considered vetted and trustworthy. Unauthorized content will be quickly and efficiently taken down. With a 99 percent takedown success rate and an estimated window of under five hours for takedowns; your brand, employees, and customers will be more secure.

Detect Threats Beyond the Perimeter

PhishLabs' Digital Risk Protection provides comprehensive visibility into the digital risks that exist outside the network perimeter. Driven by business needs, the enterprise digital footprint is ever-expanding.

Key executives are using social media. Customers are engaging via mobile devices and applications. Different departments are relying on a multitude of cloud services and platforms daily. Every expansion broadens the digital footprint, exposing the enterprise to additional risks.

These risks fall into three basic categories: impersonation, data exposure, and cyber threats.

Impersonation or spoofing exploits trust in the enterprise and its brands. Phishing sites, copycat domains, fake mobile apps, fake social media profiles, and traffic diversion schemes are a few of the many ways threat actors digitally impersonate enterprises.

Data exposure occurs when non-public, sensitive information is disclosed on a digital platform. Stolen credentials for sale on the dark web, source code pasted to an online site, and minutes from private board discussions leaked on social media are examples of data exposure risks.

Cyber threats are imminent signs that the enterprise, its digital assets, or its employees will be targeted online. Examples of this include: threats being made to hack an executive's social media account, requests on the dark web to target an enterprise, and company account login URLs being added to malware targeting configurations.

Our experts investigate activity observed across these vectors, prioritizing and focusing on the digital risks that matter most.

Gain Meaningful Context and Intelligence

With a vast and expanding digital footprint, there is simply too much information available to sort through. PhishLabs' team of experts review and analyze digital risks on your behalf, allowing your team to prioritize and focus on risks that matter the most. We maintain extensive visibility across the digital and phishing landscape.

The PhishLabs Research, Analysis, and Intelligence Division (R.A.I.D.) monitors global email, domain, social media, mobile, dark, deep, and open web activity.

We also gather data from our extensive network of partners. We investigate threats and extract meaningful intelligence on cybercrime operations and systems. This enables proactive disruption of the underlying ecosystem that supports attacks targeting our clients.

Digital Risks

Spoofing and Impersonation

- Phishing Sites
- Copycat Domains
- Fake Mobile APps
- Fake Social Media Accounts
- Traffic Diversion Schemes

Data Exposure

- Bin Numbers For Sale
- Source Code Leaks
- Stolen Credentials
- Protected Data Posted Online
- Oversharing on Social Media

Cyber Threats

- Treat Actors Discussing Plans
- Threats Made Online
- Requests to Target
- Targeting Configs Added to Malware

Vectors

- Email
- Domains
- Social Media
- Mobile Apps
- Malware
- Deep Web
- Dark Web
- Open Web

Actors

- Cybercriminals
- Nation-States
- Hactivists
- Employees/VIPS
- Vendors/Partners
- Competitors

PHISHLABS

As a managed services provider with more than 15 years of experience finding and stopping threats outside the traditional network perimeter, PhishLabs is the ideal partner to help cyber security teams protect their enterprise, brands, and customers from digital risks.

PhishLabs Managed Threat Intelligence and Mitigation services make it easier than ever to manage risks across email, domain, social media, mobile, dark, deep, and open web vectors. Our expert-driven, managed approach goes beyond do-it-yourself tools to ensure the digital risk protection outcomes enterprises want.

To learn more, visit www.phishlabs.com.

@PhishLabs

linkedin.com/company/phishlabs