Proofpoint Virtual Takedown

Reduce Consumer, Business and Employee Exposure to Malicious Domains

KEY BENEFITS

- Reduce end-user, business partner and employee exposure to malicious domains
- Automate blocklist reporting
- Apply Virtual Takedown to phishing sites, sites hosting malicious content, sites selling counterfeit goods and sites promoting criminal activity

Many of the nearly 200,000 domains registered every day[1] are used by malicious actors to attack the employees, business partners and customers of legitimate organisations. Proofpoint Virtual Takedown lets you quickly reduce user exposure to malicious domains.

Proofpoint Virtual Takedown is an optional add-on to Domain Discover. It lets you submit malicious and criminal domains, including domains engaged in phishing, propagation of malicious content, or engaged in criminal activity, to leading blocklists used by a wide array of ISPs, devices, web services and security products. Apps, services and infrastructure that subscribe to these blocklists then render the domains inaccessible at the web, DNS and/or SMTP levels. As a result, end users cannot access web content or receive email from these domains.

Quickly Prevent Access to Bad Domains

Virtual Takedown can provide quick intervention for certain types of malicious domains. This includes domains used for:

- **Phishing:** A domain hosting a web page that looks like the login page for a bank and is used to phish customer credentials
- **Malicious content:** A domain that spreads malware or exploits vulnerabilities in the user's web browser to gain access to their computer and/or install malware
- **Selling counterfeit goods:** A domain hosting a website selling counterfeit goods such as luxury fashion items or technology products
- **Criminal activity:** A domain used to conduct low-volume email attacks, such as wire transfer fraud, targeting employees and business partners

1 Proofpoint. "2019 Proofpoint Domain Fraud Report." May 2019.

Because Virtual Takedown does not take down domains at the registrar or hosting provider level, it is a faster and more cost-effective intervention. With Virtual Takedown, action can be taken in hours rather than weeks or months. What's more, Virtual Takedown can be used in conjunction with traditional takedown methods for comprehensive protection.

Act Quickly with Automated Response

Every second counts when dealing with malicious domains. Domain Discover will automatically collect the evidence required for the virtual takedown submission. You can also add notes or attach additional evidence with further context as part of the request. From there, the domain will be reviewed by Proofpoint analysts and then submitted to the applicable blocklists. Proofpoint works with a large number of blocklists that cover billions of users and devices across the internet.

LEARN MORE

For more information, visit **proofpoint.com**.