PhishBlocklist Powered by zvelo

MAKING THE INTERNET SAFER FOR ALL!

AI-POWERED

Phishing Detection

The industry's most comprehensive and effective blocklist of active and emerging phishing URLs—including zero-day threats

Phishing is the *#1 Cyber Threat* Facing Businesses and Consumers

95% of corporate network attacks and data breaches are the result of a successful phishing attack.[1]

Regardless of business size or prepared network defenses—it only requires a single errant click by one user to compromise sensitive data and infrastructure. According to IBM[2], the global average cost of a data breach now exceeds $3.86 million (USD). Even midsize companies incur an average of $1.6 million (USD) in damages for remediation efforts[3]. Phishing attacks and social engineering strategies are also growing more sophisticated, and email isn't the only threat vector you need to be concerned with. The next generation of phishing attacks are being initiated via SMS/text/messaging apps (SMiShing), voice calls (Vishing), on social media platforms, and through online advertisements. Together with other trends, like new webkits and the adoption of HTTPS encryption—which over 50% of fraudulent sites now use[4]—phishing threats are emerging with increasing effectiveness and speed. This trend is likely to accelerate in coming years with the rapid adoption and convergence of IoT and 5G technologies.

In recent years, the cybersecurity community has focused on user education, password managers, and two factor authentication (2FA) to combat the growing phishing threat. While these efforts all play a critical role in securing our networks, and continued awareness is important—they alone are unable to address the growing threat posed to increasing numbers of users and devices across web-connected apps and services. To put it simply, the cybersecurity community has been unable to provide any meaningful protection from the dangers and damage caused by phishing at large. That is... **until now.**

Introducing next-generation, AI-powered detection for phishing URLs—including zero-day threats.

PROTECT USERS AND DEVICES ACROSS YOUR NETWORKS WITH THE INDUSTRY'S MOST COMPREHENSIVE AND EFFECTIVE PHISHING DETECTION.

For over a decade, zvelo has been a pioneer in web content categorization and malicious detection. Our global, AI-powered network continuously monitors and analyzes both content and traffic from over 650 million end users worldwide. By leveraging this clickstream data and our deep understanding of both ActiveWeb content and threats—zvelo has created a comprehensive, human-annotated phishing dataset as well as custom machine learning (ML) models for phishing detection.

The result is a next-generation, AI-powered phishing detection system capable of detecting, predicting, and identifying the millions of active and emerging phishing URLs, threats, and webkits on the ActiveWeb—including zero-day threats not found on **ANY OTHER phishing feed.**

New detections are added to the zveloDB URL Database in real-time for unmatched up-to-the-minute protection for zvelo OEM partners. Alternatively, phishing detections can be used with your existing infrastructure to augment your defenses by ingesting the standalone PhishBlocklist.

USE CASES

- Web Filtering & Parental Controls
- DNS Filtering & DNS RPZ
- Email Filtering
- Antivirus Software
- Next-Generation Firewalls
- Endpoint Security
- Enterprise Network Administration
- Ideal for ISPs, Telcos, CASBs, MSSPs, SIEM, IPS, UTM Vendors, and more...

GET UNMATCHED PROTECTION FROM ZERO-DAY PHISHING THREATS

Protect your networks, devices, and users with the industry's most comprehensive and effective AI-based phishing detection.

PHISHBLOCKLIST™

Augment your network defenses against phishing URLs with the standalone **PhishBlocklist™**.

Learn more at: **phishblocklist.com**

ZVELODB™ URL DATABASE

Achieve maximum coverage from malicious AND phishing threats with the award-winning **zveloDB URL Database**.

Learn more at: **zvelo.com/phishing**

Advantages of zvelo AI Phishing Detection

AI-BASED DETECTION POWERED BY HUMAN-SUPERVISED MACHINE LEARNING & CONTINUOUS SAMPLING

By leveraging a comprehensive, human-annotated phishing dataset and human-supervised machine learning process—along with a continuous sampling and feedback loop—zvelo's AI phishing detection service continuously improves and is able to detect new threats in real-time with unmatched speed, scale, and accuracy.

CONTINUOUS, REAL-TIME IDENTIFICATION, TRACKING, AND UPDATES FOR THE MILLIONS OF ACTIVEWEB PHISHING THREATS

New threats are emerging constantly and the lifespan of phishing URLs and campaigns can vary significantly. It just isn't feasible for human analysts to keep up with accurately identifying and tracking all of these new AND evolving threats. Together, our AI/ML approach and scalable, global infrastructure are able to identify and deliver continuous updates to partners and deployments worldwide—providing up-to-the-minute protection.

Unmatched Coverage & Protection

PROTECT USERS FROM CREDENTIAL ATTACKS AND EMERGING PHISHING WEBKITS

Phishing continues to grow more sophisticated and effective year after year. Since 2011, users falling victim to phishing attacks has increased by 85%, with 56% of users clicking on phishing links within emails[5]. AI-based phishing detection helps prevent users from being compromised on the resulting web page or login form.

PROTECT USERS AGAINST BUSINESS EMAIL COMPROMISE (BEC) AND EMAIL ACCOUNT COMPROMISE (EAC)

BEC and EAC scams are two of the most significant threats facing businesses and consumers today–with losses exceeding $12.5 Billion (USD) between 2013 and 2018[6]. Mitigate risk and bolster defenses against unwanted intrusion and social engineering attacks with advanced protection against phishing URLs and campaigns.

COMPREHENSIVE, DEVICE-AGNOSTIC PHISHING PROTECTION

Users are 3x more likely to fall for phishing on a mobile device than a desktop[7]. Phishing continues to evolve and target devices other than those covered by traditional network security frameworks (i.e. desktops and laptops). Umbrella-level network protections and device-agnostic security are critical in preventing compromises caused by phishing attacks.

PROTECT USERS FROM PHISHING ATTACKS LEVERAGING TOP TARGETED BRANDS

Dropbox, PayPal, Google, Amazon, Wells Fargo, Apple, Facebook, and more. Phishing lures and webkits routinely impersonate high-profile and reputable brands (particularly in tech, retail, and finance), deceiving users into inadvertently handing over their credentials. The zvelo phishing detection AI/ML models have been carefully trained to identify emerging threats that leverage the industry's most targeted brands—providing critical protection against these highly effective tactics. **Are your users targeted by phishing attacks?**

OEM BENEFITS

- Protect users and devices with unparalleled AI-based identification of active and "zero-day" phishing threats
- The industry's most comprehensive and effective defense against phishing threats
- Flexible deployment options for easy integration
- Support for over 200 languages
- Continuously detects and tracks millions of phishing URLs in real-time

KEY FEATURES

- Real-time detections powered by the ActiveWeb clickstream data from 650M+ end users worldwide
- Powered by zvelo's AI-based phishing detection service, part of the zveloAI Cloud Network
- Detects and tracks millions of emerging phishing URLs, webkits, and campaigns
- Updated hourly for maximum protection against zero-hour and zero-day phishing threats

Email us at **sales@zvelo.com**

LEARN MORE

PHISHBLOCKLIST™ | POWERED BY ZVELO

PhishBlocklist offers the industry's most effective and comprehensive protection from active and emerging phishing URLs. Powered by zvelo, the leading provider of web content categorization, URL database, malicious and phishing detection, as well as other data services—PhishBlocklist is trusted OEM partner for many of the market's preeminent Network Security vendors, zvelo services help protect over 650 million end users worldwide and deliver industry-leading coverage, accuracy, protection, and understanding of the ActiveWeb.

[1] According to the Sans Institute, only 5 percent of attacks begin come from other sources or tactics (https://www.sans.org/)
[2] According to a 2018 study by IBM Security and the Ponemon Institute (https://www.ibm.com/security/data-breach/)
[3] Found in the 2017 Enterprise Phishing Resiliency and Defense Report by PhishMe/Cofense (https://cofense.com/resources/)
[4] In Q3 2018, nearly 50% of phishing sites are using HTTPS. 40% more than Q2 and a 900% increase over 2016 (https://www.proofpoint.com)
[5] Users falling victim to phishing has increased by 85% since 2011, with 56% of users clicking on links within phishing email. (www.lookout.com)
[6] 2018 FBI report detailing losses between Oct 2013 and May 2018 exceeded $12.5 Billion (USD). (https://www.ic3.gov/media/2018/180712.aspx)
[7] Mobile users accessing phishing sites are 3x more likely to submit login info than desktop users (https://securityintelligence.com)

POWERED BY

zvelo
We Categorize the Web®