



# Remote User Phishing Protection

Anywhere zero-hour protection against the broadest range of phishing threats.

SlashNext remote user phishing protection solutions enable IT security teams to arm their endpoints with the industry's strongest protection against zero-hour phishing threats. Regardless of phishing attack vector (email, SMS, social media, messaging apps, games, ads, pop-ups, search, technical scams, SMSing, etc.), SlashNext protects users from browsing to malicious sites. This disrupts phishing and social engineering threats near the start of the killchain, dramatically reducing the risk of credential theft, technical scams, SMSing, malware infection, and breaches.

## Uniquely Effective Endpoints that Focus on Phishing Threats

Unlike other endpoint security vendors, SlashNext is entirely focused on phishing. More powerful phishing site detection technology protects users from more advanced threats, many of which currently bypass other security controls and "safe browsing" features. This protects users against all six major categories of phishing and social engineering threats:



### Credential Stealing

Fake login pages, account takeover, etc.



### Tech Support Scams

Scareware, fake virus alerts, pop-ups, on-line support scams, etc.



### Document Theft

Weaponized documents, IP, media theft, etc.



### Money Transfer Scams

Credit card and Bitcoin fraud, wire transfers, fake deals, loan and gift card scams, etc.



### Rogue Software

Rogue apps, browser extensions, fake AVs, etc.



### Phishing Callbacks (C2s)

Data exfiltration, C2 callbacks, etc.

## Browser and Mobile App Deployment Options

Two SlashNext remote user phishing protection solutions are available to deploy. Mobile Phishing Protection protects iOS and Android users from mobile-centric phishing threats with a lightweight, cloud-powered app. Browser Phishing Protection shields employees from live phishing sites with a lightweight browser extension that augments endpoint security solutions on Windows, MacOS, Chrome OS, and Linux machines.

### Lightweight browser extensions



Chrome



Firefox



Safari



Edge

### Lightweight mobile apps



Android



iOS

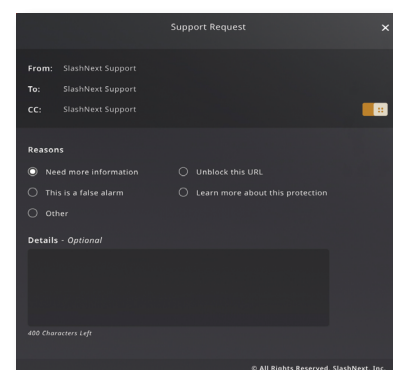
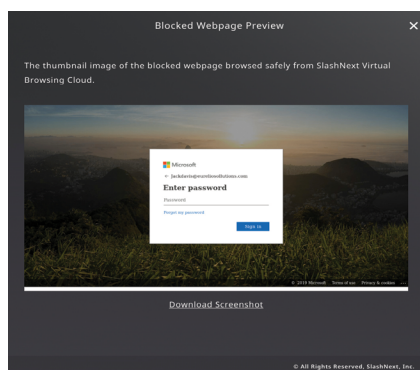
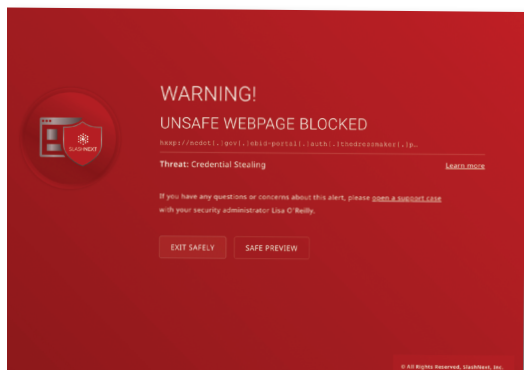
Each solution delivers the same proven anti-phishing capabilities with a simple, intuitive user experience.

## THE SLASHNEXT ADVANTAGE

- **Anywhere, Anytime Protection:** 24x7 automated phishing focused protection and reporting, reduces threat exposure for remote users.
- **All Endpoint Types:** Desktops, laptops, iOS and Android tablets/phones (BYOD and company-owned).
- **Multi-Vector Protection:** Blocks threats from links in phishing emails, SMS/text, social media, messaging apps, rogue apps, pop-ups, ads, Web, and more.
- **Comprehensive Protection:** Blocks multi-payload threats from all six major categories of phishing.
- **SMSing Protection:** Blocks and alerts users to SMS phishing texts.
- **Educational Warning Page:** Details on phishing threat and Safe Preview.
- **No PII or Privacy Risks:** Protection that doesn't violate user privacy or transmit sensitive personal data.
- **Handles Encryption Challenges:** Protection that works with new encryption (TLS 1.3, DNS over HTTPS).
- **Cloud-Based Reporting:** Real-time notifications and alerts for security admin reporting.
- **Intuitive User Interface:** Simple, easy-to-use, automated phishing detection and blocking.
- **Easy to Use, Lightweight:** Efficient operation has negligible impact on mobile device performance and battery usage.
- **Easy Deployment & Management:** Works with UEM solutions, SSO providers, and SlashNext Endpoint Management System.

## Browser Warning and Safe Preview Screens

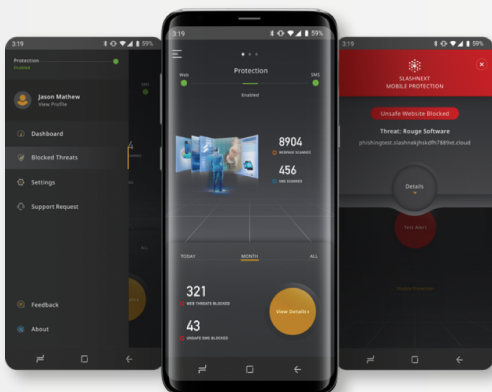
Users who attempt to browse to a malicious site are blocked and receive an informative warning page allowing them to access a Safe Preview screen shot of the blocked page along with very useful information about the threat. They can also report and request support on the incident.



## Simple Reporting and Administration

Security administrators can receive real-time phishing incident alerts via email, plus a daily summary report. A simple-to-use Endpoints Management Systems from SlashNext, makes it easy to manage groups, policies, users, and licenses. Users and groups can be easily created, assigned, invited, and provisioned manually or directly imported through a CSV file.

SlashNext Mobile Phishing Protection can also be deployed and managed through popular third-party enterprise EUM solutions across enterprises of all sizes. They also integrate with leading SSO solutions for simpler user provisioning and management.



## Remote User Phishing Protection for Android and iOS

For iOS and Android, protection goes one step further by intercepting and quarantining SMS phishing messages. Regardless of the version used, SlashNext does not access or store any PII, so personal data always remains safe. Highly efficient background operation of these products minimizes memory and battery usage, enabling SlashNext Mobile Phishing Protection to seamlessly operate along side other endpoint AV solutions.

## Better Detection = Better Protection

SlashNext remote user phishing solutions are powered by updates from the industry's broadest, most-up-to-the-minute phishing threat intelligence. Using cloud-scale, massive computing power, pre-emptive threat hunting, and a global sensor network, SlashNext inspects billions of Internet transactions and millions of suspicious URLs daily to detect emerging zero-hour threats.

Phishing site detection is based on SlashNext patent-pending SEER™ threat detection technology. SEER launches browsers in a purpose-built cloud to dynamically inspect page contents and server behavior using advanced computer vision, OCR, and natural language processing. With more clues and real-user like interaction dynamics, SlashNext detects threats that evade URL inspection and domain reputation analysis methods. It is also able to identify and follow shortened links (such as bit.ly), multiple URL re-directs, and detect phishing pages hosted on compromised websites or legitimate infrastructure.

## Learn More about SlashNext Anti-Phishing and IR Solutions.

Request a demo today at [www.slashnext.com/request-a-demo](http://www.slashnext.com/request-a-demo)