Phishing and spear phishing attacks are now aimed at organizations of all sizes, and are a preferred method cybercriminals use to breach networks. Phishing analysis by F5 Labs and Webroot shows that, during July 2019, 54% of malware domains leveraged HTTPS. Phishers are playing on the trust users have of the green lock as another way to make their URLs seem legitimate.\(^1\) Phishing attacks are so sophisticated, they often fool IT security professionals.

### Stopping Phishing Attacks in Their Tracks

The BrightCloud® Real-Time Anti-Phishing Service crawls potential phishing links and determines their risk level in real time, helping prevent security breaches and data loss by leveraging advanced machine learning and content classification to automate phishing detection.

Real-time URL validation is the only truly effective protection against zero-hour phishing attacks, disguised redirection, and recently hijacked websites. The BrightCloud Real-Time Anti-Phishing Service catches advanced phishing attacks by providing time-of-need protection through real-time scans immediately before sites are visited.

*In 2019, phishing URLs encountered grew by 500%.\(^2\)*
Add-on BrightCloud Threat Insights for the Real-Time Anti-Phishing Service for supplementary information on phishing URLs. This includes:

» Identifying the target of the phishing site so users can identify patterns in attacks and focus their analysis
» A snapshot of the phishing site when it was live to enable customers to see what the site looked like
» Additional data on the URL used for the phishing attack
» Searching for phishing URLs that attempt to imitate a specific brand or website

Partner Benefits

» Differentiate yourself from your competition
Offer highly accurate, next-generation, real-time protection against phishing attacks

» Leverage the Webroot Platform
Harness the world’s most powerful cloud-based security analysis engine

» Easy to integrate, easy to use
Simple integration into your solution via RESTful API and an SDK

» Minimal impact on user experience
Sites are scanned in real time to provide advanced protection with minimal user interruption

BrightCloud Real-Time Anti-Phishing Service in Action

Whenever users access the internet, the BrightCloud Real-Time Anti-Phishing Service can protect them from accidentally compromising their accounts or picking up malware or ransomware from malicious sites. Additionally, this service can be integrated to:

» Improve web security for network appliances
» Identify new zero-hour threats for anti-fraud services
» Provide safe web browsers and plugins
» Enhance email filtering software and endpoint security products
» Filter user generated content in social networks, blogs, and messaging apps

Integration Options

Webroot provides a RESTful web service, as well as an SDK, allowing technology partners to incorporate the BrightCloud Real-Time Anti-Phishing Service into their own solutions with ease. Additionally, this service combines with existing security solutions through the same SDK as other BrightCloud services, making integration as simple and straightforward as possible.

About Webroot

Webroot, an OpenText company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.