Webroot analysis showed that in 2016, the majority of phishing sites’ life spans ranged from as low as 15 minutes to under 15 hours. Real-time URL validation is the only truly effective protection against zero-hour attacks, disguised redirection, and recently hijacked websites. The BrightCloud® Real-Time Anti-Phishing Service protects users by ensuring they visit only the websites they intend to interact with. Sites are verified at the time of the request to ensure they are legitimate and safe.

Stopping Phishing Attacks in Their Tracks

The BrightCloud Real-Time Anti-Phishing Service identifies and stops advanced phishing attacks, helping prevent security breaches and data losses. The service leverages advanced machine learning and content classification to automate the detection of phishing sites. In extensive testing, this new approach detects phishing sites three to five days ahead of the competition—a major breakthrough in the defense against phishing attacks. These sites are typically live very briefly to avoid detection by other anti-phishing technologies, so early detection is critical.

The service crawls and evaluates requested URLs in milliseconds using hundreds of site attributes as well as external factors associated with the site. This includes correlated intelligence from the contextual analysis engine, such as web reputation, IP reputation, how long the site has been in existence, recent threat history, etc. The service returns a risk score for each requested URL.

Most phishing sites are live for less than 15 hours.¹
Add-on Anti-Phishing Threat Insights provide supplementary information on phishing URLs. This includes:

- Identifying the target of the phishing site so that 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

**Partner Benefits**

- Differentiate yourself from your competition
  Offer highly accurate, next-generation, real-time protection against phishing attacks
- Leverage the Webroot® Threat Intelligence 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 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 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.