OpenDNS® 2010 Report
Web Content Filtering and Phishing

Introduction

OpenDNS® is the largest global DNS service for consumers, schools and businesses:

- Resolves 30 billion DNS queries per day
- Services 15 million requesting IP addresses per day. Many of these represent organizations with thousands of individual users
- Handles DNS for 1 percent of all Internet users worldwide

OpenDNS, a pioneer and leader in the Security as a Service space is also the leading provider of DNS-based security and infrastructure services. We enable consumers, schools, small businesses, enterprises and other organizations to secure their networks from online threats, reduce costs and enforce Internet-use policies via the following services:

- Web content filtering
- Malware, botnet and phishing protection

From this global vantage point, OpenDNS has an unprecedented view into the behaviors of Internet users. In this report, we review some of the highlights of 2010 with regard to phishing and web content filtering.

Web Content Filtering

Content may be filtered by category or by blocking specific websites via blacklisting or by allowing specific websites via whitelisting.

Top Ten Blocked Categories

Not surprisingly, the top ten most blocked categories are focused on providing a safer Internet experience for students and children, and a more work-appropriate environment for businesses. Percentages indicate the proportion of networks using category blocking that reference a given category.

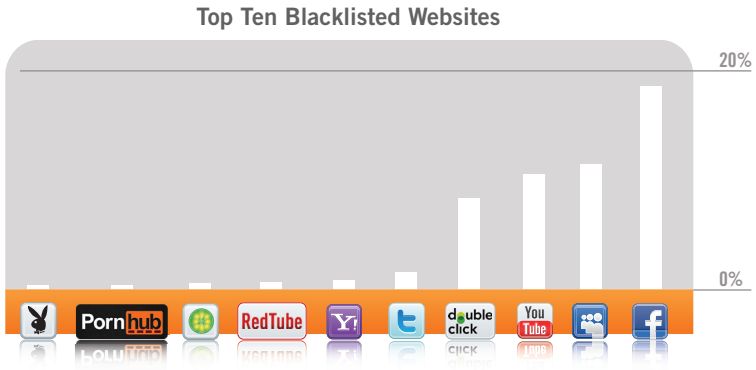
1. Pornography — 85%
2. Sexuality — 80.1%
3. Tasteless — 77.3%
4. Proxy/Anonymizer* — 76.2%
5. Adware — 69%
6. Nudity — 67.2%
7. Hate/Discrimination — 58.7%
8. Lingerie/Bikini — 58.5%
9. Gambling — 58%
10. Drugs — 57.3%

* Websites that allow users to hide their identity or circumvent the Web content filtering set up on their networks.

Top Ten Blacklisted Websites

Blacklists are typically used when there is no desire to block an entire category in principle, but there is a focus on preventing traffic to specific websites based on a combination of their popularity and content. This top ten list suggests a concern with the use of bandwidth by streaming sites and with privacy concerns from advertising networks. Percentages indicate the proportion of networks using blacklisting that reference a given site.

1. Facebook.com —14.2%
2. MySpace.com — 9.9%
3. YouTube.com — 8.1%
4. Doubleclick.net — 6.4%
5. Twitter.com — 2.3%
6. Ad.yieldmanager.com — 1.9%
7. Redtube.com —1.4%
8. Limewire.com — 1.3%
9. Pornhub.com —1.2%
10. Playboy.com — 1.2%



© OpenDNS 2011 Source: Sample of OpenDNS networks using blacklisting in 2010. n =203,399

Top Ten Whitelisted Websites

Whitelists are typically used when there is a desire to block entire categories, but access to selected websites is granted on an exception basis. These sites represent the most trusted sites in their category. The fact that many of the same sites that appear on the Top Ten Blacklisted Websites list appear on the list below may indicate the diverse perspectives people have regarding many of these sites. Percentages indicate the proportion of networks using whitelisting that reference a given site.

1. YouTube.com — 12.7%
2. Facebook.com — 12.6%
3. Gmail.com — 9.2%
4. Google.com — 9%
5. Translate.Google.com — 6.3%
6. LinkedIn.com — 6%
7. MySpace.com — 4.7%
8. Skype.com — 4.6%
9. Deviantart.com — 4.3%
10. Yahoo.com — 3.9%

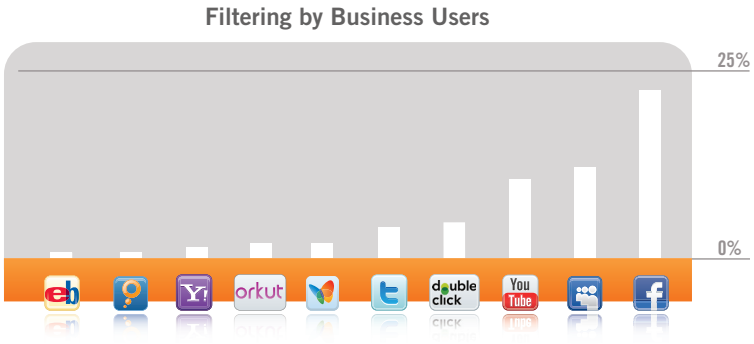
© OpenDNS 2011 Source: Sample of OpenDNS networks using whitelisting in 2010. n =262,762

OpenDNS

Filtering by Business Users

Businesses have specific goals in mind when blocking websites. They need to ensure compliance with HR policies, while also increasing worker productivity by preventing what they consider to be employee cyberslacking. This list shows that businesses are concerned with singling out popular sites considered to be of little value in a work setting, especially if they consume a lot of bandwidth. Percentages indicate proportion of business networks using blacklisting feature that reference a given site.

1. Facebook.com — 23%
2. MySpace.com — 13%
3. YouTube.com — 11.9%
4. Ad.Doubleclick.net — 5.7%
5. Twitter.com — 4.2%
6. Hotmail.com — 2.1%
7. Orkut.com — 2.1%
8. Ad.Yieldmanager.com — 1.8%
9. Meebo.com — 1.6%
10. eBay.com — 1.6%



© OpenDNS 2011 Source: Sample of OpenDNS business networks using whitelisting in 2010. n = 31,623

Phishing

OpenDNS created and runs PhishTank®, the free community Web site where anyone can submit, verify, track and share phishing data. Launched in October 2006 to coincide with National Cyber Security Awareness Month, the site employs a sophisticated voting system that requires the community to vote "phish" or "not phish," reducing the possibility of false positives and improving the overall breadth and coverage of the phishing data. Today, PhishTank is the most important phishing database available and is used by the world's largest companies. More than 1 million phishes have been submitted and voted on by the PhishTank community of researchers, academics and security experts.

Top Targets of Phishing Websites in 2010

The most frequently spoofed website in every month of 2010 was PayPal. PayPal was targeted nine times more frequently than the next most frequent target, Facebook. Five of the most targeted brands — Facebook, World of Warcraft, Sulake Corporation, Steam and Tibia — are associated with online and social games. Percentages indicate the proportion of phishing sites verified in 2010 and associated with a given target.

1. PayPal — 45.9%
2. Facebook — 5.3%
3. HSBC Group — 4.1%
4. World of Warcraft — 3.2%
5. Internal Revenue Service — 3%
6. Bradesco — 1.9%
7. Orkut — 1.7%
8. Sulake Corporation — 1.5 %
9. Steam — 1.2%
10. Tibia — 1%

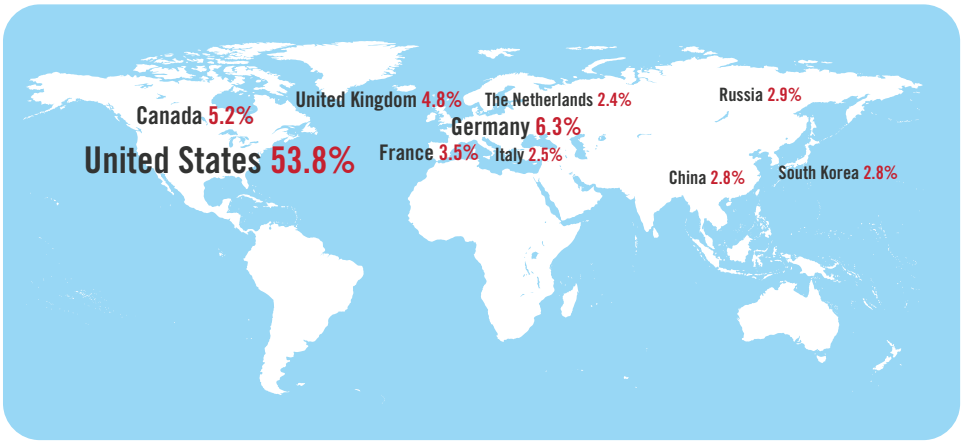
© OpenDNS 2011 Source: Sample of phishing sites tracked by PhishTank and OpenDNS in 2010. n = 117,102

Top Countries Hosting Phishing Websites in 2010

The vast majority of phishing websites were hosted in the United States — more than 60,000 separate attempts came from websites hosted in the U.S. Percentages indicate the proportion of phishing sites verified in 2010 hosted in a given country.

1. United States — 53.8%
2. Germany — 6.3%
3. Canada — 5.2%
4. United Kingdom — 4.8%
5. France — 3.5%
6. Russia — 2.9%
7. China — 2.8%
8. South Korea — 2.8%
9. Italy — 2.5%
10. The Netherlands — 2.4%

Top Countries Hosting Phishing Websites in 2010



© OpenDNS 2011 Source: Sample of phishing sites tracked by PhishTank and OpenDNS in 2010. n = 117,102

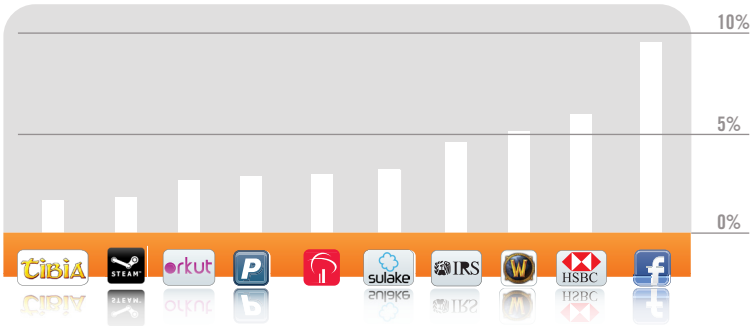
Phishing Update

One of the reasons PayPal, Inc. is so prevalent as a target in PhishTank is because PayPal uses the PhishTank API to automatically submit any phish they find to PhishTank. This is a good thing — it puts data into PhishTank quickly so the community can verify the sites and PhishTank data feed subscribers can protect their users. While this highlights the frequency that PayPal is a target, it also skews the data to make it appear that PayPal is the most phished brand, simply because they are the most vigilant in submitting data to PhishTank. Obviously, this was not our intent. We are updating the report to show the most targeted brands in 2010 with the PayPal API data removed from the dataset as nearly all other submissions come from the tens of thousands of PhishTank individual contributors.

If the PayPal API-based submissions to PhishTank are removed from the dataset of phished brands, the list of most-targeted brands in 2010 shifts dramatically:

1. Facebook — 8.64%
2. HSBC Group — 6.73%
3. World of Warcraft — 5.35%
4. Internal Revenue — Service 4.87%
5. Sulake Corporation — 3.21%
6. Bradesco — 3.15%
7. PayPal — 3.03%
8. Orkut — 2.9%
9. Steam — 1.95%
10. Tibia — 1.72%

Top Targets of Phishing Websites in 2010



© OpenDNS 2011 Source: Sample of phishing sites tracked by PhishTank and OpenDNS in 2010. n = 72,404

OpenDNS, Inc
410 Townsend St, Suite 250
San Francisco, CA 94107

Question, comments or ideas? Contact: Press@OpenDNS.com

Follow us on Twitter: @OpenDNS