

# Phishing Activity Trends Report

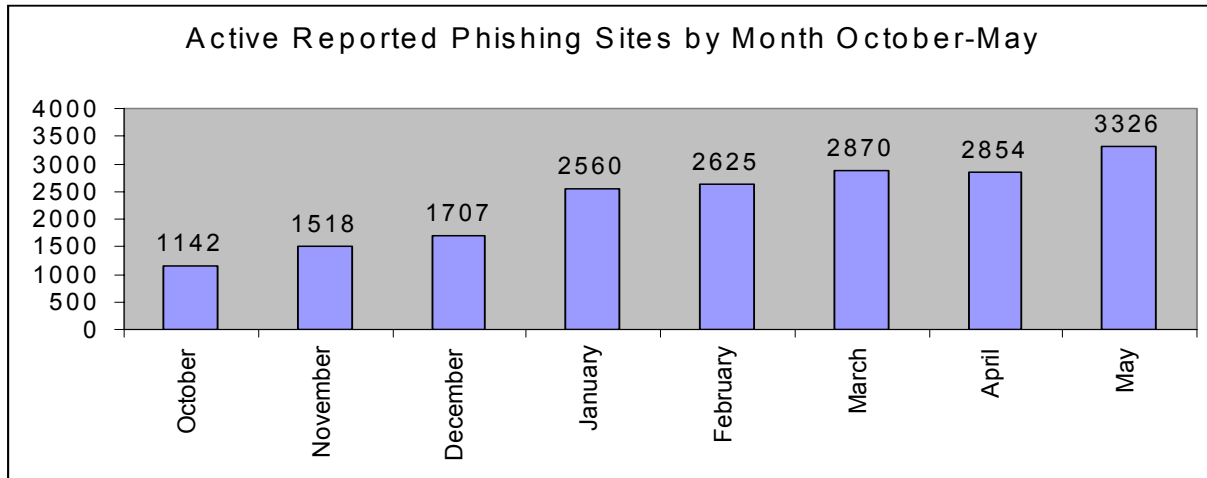
May, 2005

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince recipients to respond to them. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss.

The Phishing Activity Trends Report analyzes phishing attacks reported to the Anti-Phishing Working Group (APWG) via the organization's website at <http://www.antiphishing.org> or email submission to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org). The APWG phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing activity.

## Highlights

- Number of active phishing sites reported in May: **3326**
- Number of brands hijacked by phishing campaigns in May: **107**
- Number of brands comprising the top 80% of phishing campaigns in May: **7**
- Country hosting the most phishing websites in May: **United States**
- Contain some form of target name in URL: **46%**
- No hostname just IP address: **42%**
- Percentage of sites not using port 80: **8 %**
- Average time online for site: **5.8 days**
- Longest time online for site: **30 days**

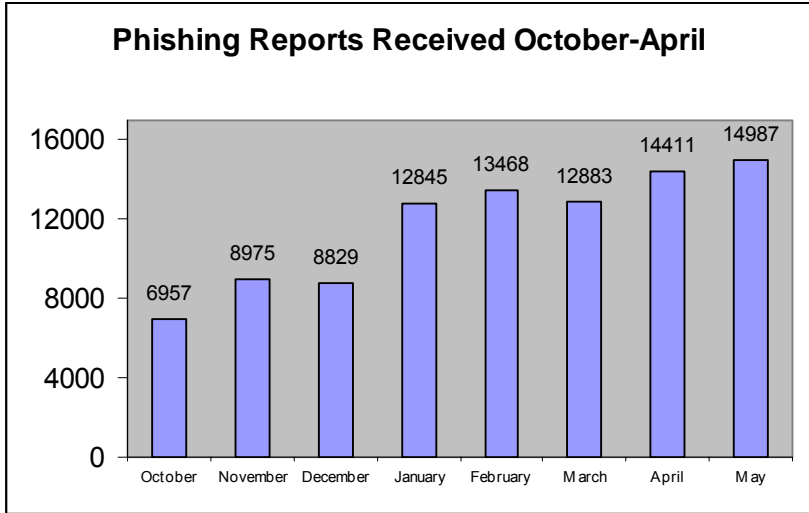


The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact Ronnie Manning at [rmanning@websense.com](mailto:rmanning@websense.com) or 858.320.9274 or APWG Secretary General Peter Cassidy at 617.669.1123. Analysis for the **Phishing Attack Trends Report** has been donated by the following companies:



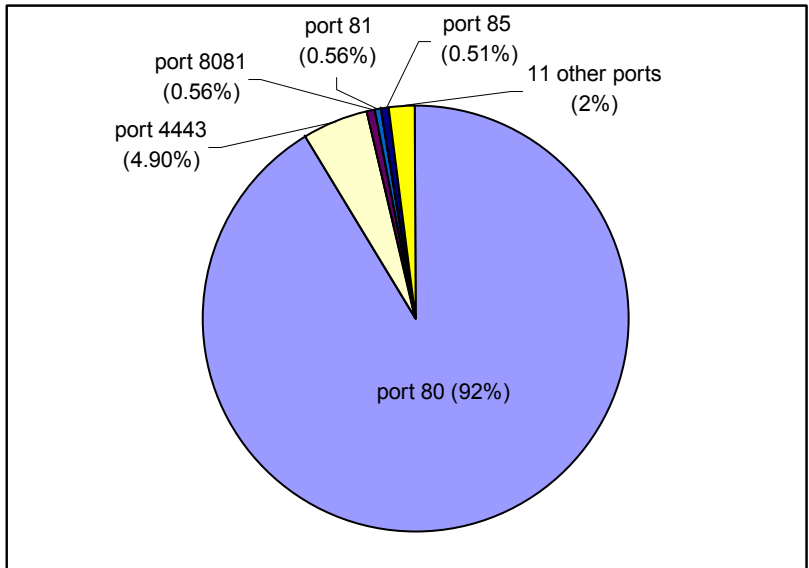
**Email Phishing Attack Trends**

The number of reports received in May was 14,978, continuing a trend of slight growth during 2005.



**Top Used Ports Hosting Phishing Data Collection Servers**

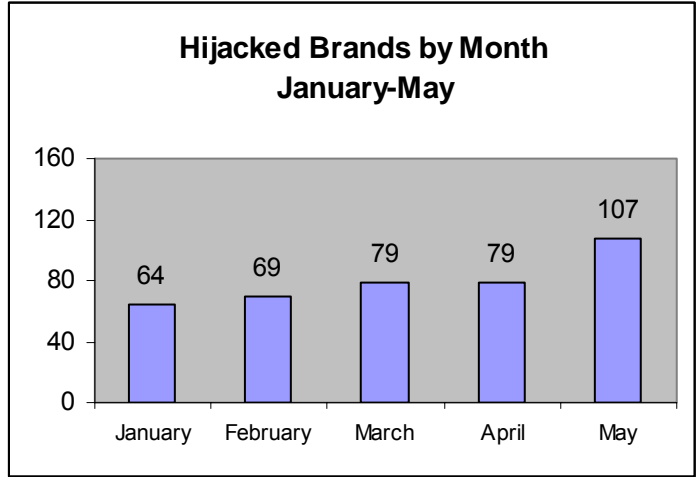
May saw a continuation of a trend of using cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at 92% of all phishing sites reported.



## Brands and Legitimate Entities Hijacked By Email Phishing Attacks

### Number of Reported Brands

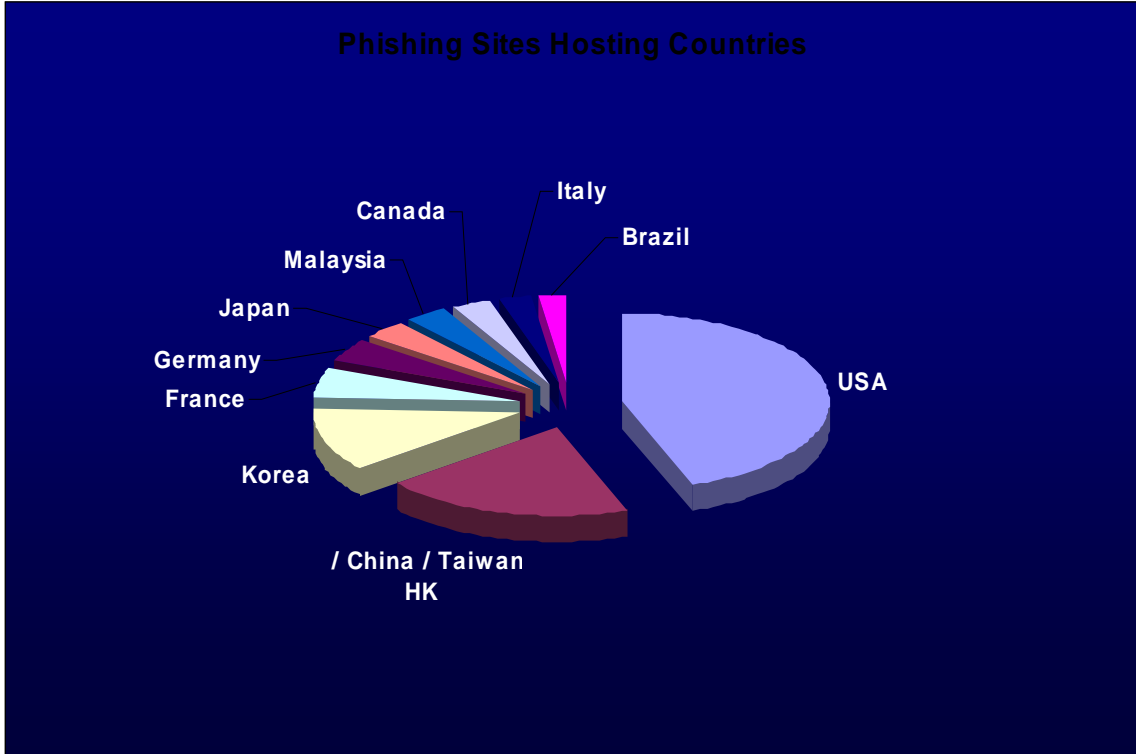
In May, the number of reportedly phished brands grew much higher than April. Seeing a major increase in the number of small and local credit unions.



## Web Phishing Attack Trends

### Countries Hosting Phishing Sites

Numbers in China declined for the first time since we have been recording countries. USA 34%, China 15 %, Korea 9 %, France 3.94%, Germany 3.3% , Japan 2.6%, Malaysia 2.6% , Canada 2.3 % , Italy 2.02% , Brazil 1.6% . This month had a total of 64 unique countries that were hosting phishing sites.



## Phishing Research Contributors



### Tumbleweed Message Protection Lab

The mission of the Tumbleweed Message Protection Lab is to analyze current and emerging enterprise email threats, and design new email protection technologies.

Lead investigator:  
John Thielens, johnt@tumbleweed.com



### Websense® Security Labs™

Websense Security Labs mission is to discover, investigate, and report on advanced Internet threats to protect employee computing environments.

Lead investigator:  
Dan Hubbard, dhubbard@websense.com

For media inquiries please contact Ronnie Manning at [rmanning@websense.com](mailto:rmanning@websense.com) or 858.320.9274 or Peter Cassidy, APWG Secretary General at 617.669.1123.

### About the Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement.

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are nearly 900 companies and government agencies participating in the APWG and nearly 1400 members. Note that because phishing attacks and email fraud are sensitive subjects for many organizations that do business online, the APWG has a policy of maintaining the confidentiality of member organizations.

The website of the Anti-Phishing Working Group is <http://www.antiphishing.org>. It serves as a public and industry resource for information about the problem of phishing and email fraud, including identification and promotion of pragmatic technical solutions that can provide immediate protection and benefits against phishing attacks. The analysis, forensics, and archival of phishing attacks to the website are currently powered by Tumbleweed Communications' Message Protection Lab.

The APWG was founded by Tumbleweed Communications and a number of member banks, financial services institutions, and e-commerce providers. It held its first meeting in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its steering committee, its board and its executives.