# Anti-Phishing Working Group

## Phishing Attack Trends Report January, 2004

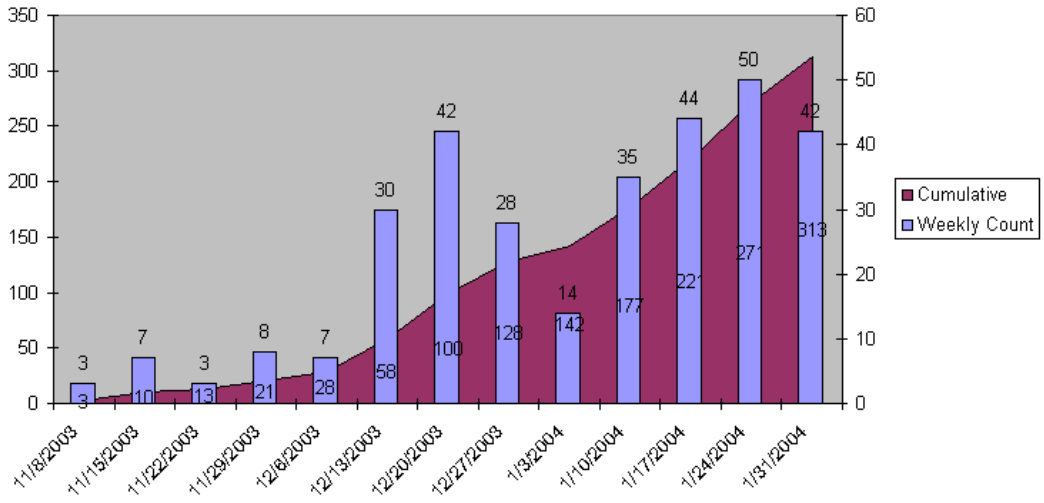
Phishing attacks involve the mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. These fraudulent messages are designed to fool the recipients into divulging personal authentication data such as account usernames and passwords, credit card numbers, social security numbers, ATM card PINs, etc. Because these emails look "official" and recipients trust the brand, they often respond to them, resulting in financial losses, identity theft, and other fraudulent activity.

The Phishing Attack Trends Report analyzes phishing attacks reported to the Anti-Phishing Working Group via the organization's website, http://www.antiphishing.org or email submission via reportphishing@antiphishing.org. The Anti-Phishing Working Group phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing attacks.

## Highlights

- Number of unique phishing attacks reported in January: **176**
- Percent of phishing attacks reported in January that were 'repeats': **13.6%**
- Organization most targeted by phishing attacks in January: **eBay**
- Business sector most targeted by phishing attacks in January: **Financial Services**
- Percent of phishing attacks in January using the Microsoft IE browser exploit: **7.8%**

**Unique Phishing Attack Trend**
**Nov 2003 - Jan 2004**




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 Dan Maier at dmaier@antiphishing.org or +1 650-216-2078.

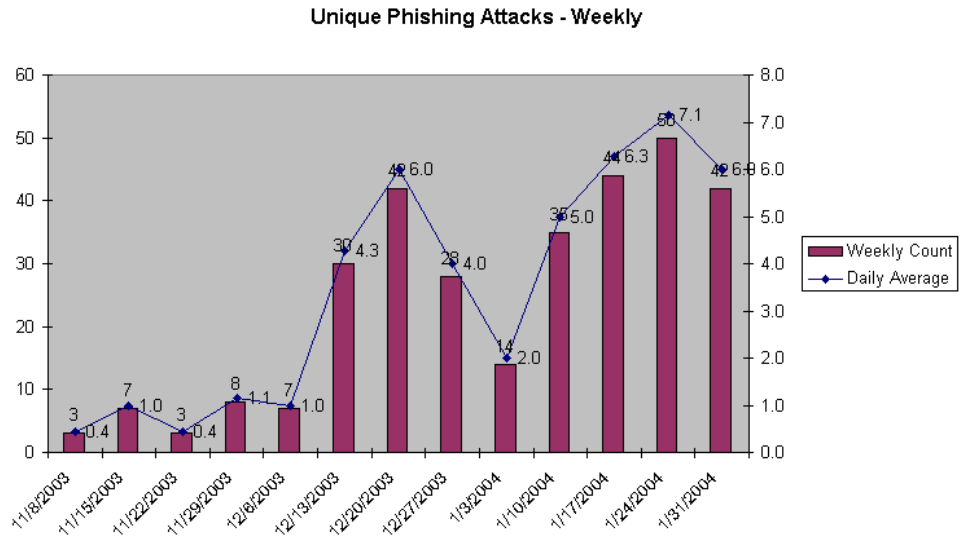
Analysis for the **Phishing Attack Trends Report** has been donated by the Tumbleweed Communications Message Protection Lab. The mission of the Tumbleweed Message Protection Lab is to analyze enterprise email threats (e.g. spam, email fraud, viruses, etc) and design new email protection technologies.

TUMBLEWEED COMMUNICATIONS

# Anti-Phishing Working Group

## Email Phishing Attack Trends

In January, there were 176 new, unique phishing attacks reported to the Anti-Phishing Working Group. This was a 52% increase over the number of attacks reported in December (116). While the average number of phishing attacks per day in January was 5.7, analyzing this information on a weekly basis shows an increasing trend with a peak of 7.1 attacks per day in the third week of January.




Note that while "phishers" appeared to take a break for their New Year celebrations, the volume of phishing attacks in January has increased above the volumes seen during the Christmas holidays in December. in addition to the increasing volume, we are starting to see a number of phishing attacks that are "repeats" – these attacks were sent out previously, and identical version of these attacks appear to have been sent out again. Over 13% of the attacks in January were 'repeats' seen in previous months.

## Who Is Being Targeted?

### Most-Targeted Companies

The most targeted companies in January were largely similar to those targeted in previous months. eBay once again was the most targeted company, with 51 unique attacks that hijacked eBay's brand. This represents a 50% growth in attacks from the number seen in December (33). Citibank was the second most attacked company in January with 35 unique attacks hijacking its brand, taking over second place on the list with more than 100% growth in attacks. And coming in a close third was AOL (35 attacks), which also experienced over 100% growth in reported attacks.

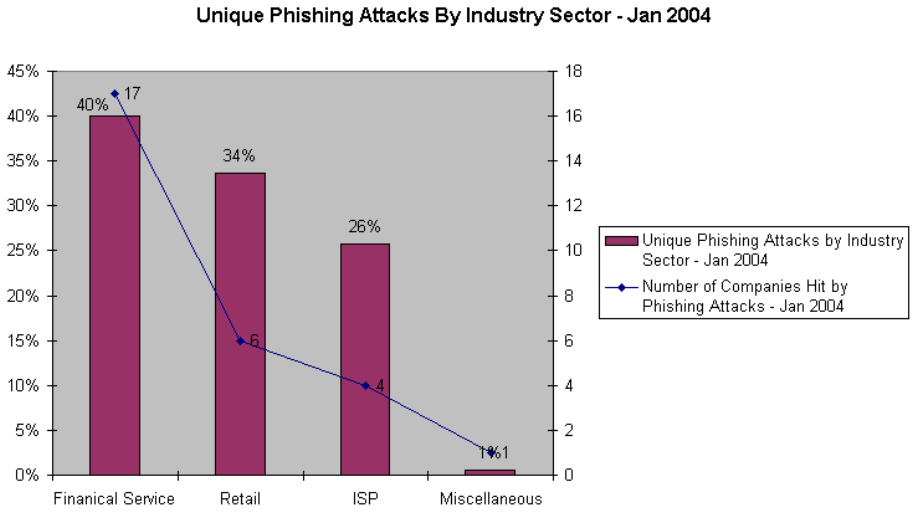
**Unique Phishing Attacks by Targeted Company**

| PhishTarget | Jan 2004 | Dec 2003 | Nov 2003 |
|---|---|---|---|
| eBay | 51 | 33 | 6 |
| Citibank | 35 | 17 | 6 |
| AOL | 34 | 16 | 4 |
| Paypal | 10 | 6 | 4 |
| Earthlink | 9 | 4 | 2 |
| American Express | 6 | 4 | 1 |
| Microsoft | 3 | 3 | 1 |
| Visa | 2 | 2 | 1 |
| Westpac | 2 | 2 | 1 |
| ANZ | 2 | 2 | 1 |
| Fleet Bank | 2 | 2 | 1 |
| National Australia Bank | 2 | 1 | 0 |
| Yahoo | 2 | 1 | 0 |
| Amazon.com | 1 | 1 | 0 |
| AT&T | 1 | 1 | 0 |
| Barclays | 1 | 1 | 0 |
| Commonwealth Bank | 1 | 1 | 0 |
| Credit Card | 1 | 1 | 0 |
| E-Gold | 1 | 1 | 0 |
| FDIC | 1 | 1 | 0 |
| Lloyds | 1 | 1 | 0 |
| Sears | 1 | 1 | 0 |
| SwiftPay | 1 | 1 | 0 |
| US Bank | 1 | 1 | 0 |

# Anti-Phishing Working Group

### Most-Targeted Industry Sectors

The most targeted industry sector for phishing attacks continues to be Financial Services, closely followed by the Retail sector (primarily online retailers). Note that while more Financial Services companies have been targeted than any other sector, companies in the Retail and ISP sectors have more often been the target of multiple unique attacks.




## Website Spoofing Trends

The majority of phishing attacks use a link to a website as their "call to action", although a few attacks ask the recipient to download a file (that generally contains a virus or Trojan program). There are several techniques used by "phishers" to disguise the fact that the website to which they are taking their victim is not authentic:

1. **"Cousin" URLs**
   These Web addresses look/sound like authentic URLs, but the domains are actually registered to scammers. Examples of these fraudulent websites include:
   - http://account-security-ebay.servepics.com/
   - http://aol-wallet.com
   - http://www.anz-billing.co.nz
   - http://www.aol-termsofservice.com
   - http://www.ebay-secure.com
   - http://www.yahoo-billing.com

   These types of Web addresses are used in 9.3% of the unique phishing attacks that were reported for January.

2. **URLs that exploit URL syntax for user authentication**
   Microsoft's Internet Explorer browser supports the ability to send usernames and passwords to a server in the format "*http(s)://username:password@domain.com/file.html*". This allows a scammer to use this URL syntax to create a link in a phishing email that appears to open a legitimate website, but actually opens a deceptive ("phishing") website. For example, "*http://validbank.com@phishersite.com/getinfo.html*" takes the user to "*phishersite.com*", even though it may look to the user like they are going to "*validbank.com*". Depending on what version of browser the user has, the Web address may show up as either "*http:// phishersite.com/getinfo.html*" or "*http://validbank.com@phishersite.com/getinfo.html*".

   These types of Web addresses are used in 32% of the phishing attacks reported for January.

3. **URLs that exploit a Microsoft Internet Explorer URL display flaw**
   On December 9, Secunia (a Danish security firm) announced that they had identified a vulnerability in Microsoft's Internet Explorer browser that could be exploited by malicious people to display a fake URL in the browser's address bar and status bar (http://secunia.com/advisories/10395/). The vulnerability is exploited by including "%01" or "%00" before the "@" character in a URL using the "user authentication" syntax described in item 2. above. When these characters are inserted, the browser displays the URL to the left of these characters, while actually taking the user to the domain to the right of the "@" character. For example, the following URL was used in the U.S. Bank phish: "*http://www.usbank.com%01@bos.es.kr/index.htm*". While the user's browser would show *http://www.usbank.com*" in the address bar, the actual site that the user is taken to is "*http://bos.es.kr/index.htm*", a phisher website hosted somewhere in South Korea.

   We saw the first phishing attack utilizing this IE exploit reported on December 18, 2003 (against Visa), 9 days after Secunia announced it. Since that time, we have seen the exploit used in 7.8% of unique phishing attacks reported.

4. **Download Trojans and keyloggers**
   A small number of phishing attacks include a Trojan attachment in the message that recipients are encouraged to download and run. These Trojans generally contain keylogger programs that silently monitor the victim's computer for patterns of keystrokes that look like credit card numbers or social security numbers, or for new windows that open containing the name of a bank or credit card company. The program captures the typed information to a text file, and then uses a built-in email system to send the contents to an email dropbox for collection.

   We've seen this approach used in 5 phishing attacks in January (2.8%). Note however that this is up from the 1 such attack seen in December.

**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. 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 Web site 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 Web site 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.