Anti-Phishing Working Group

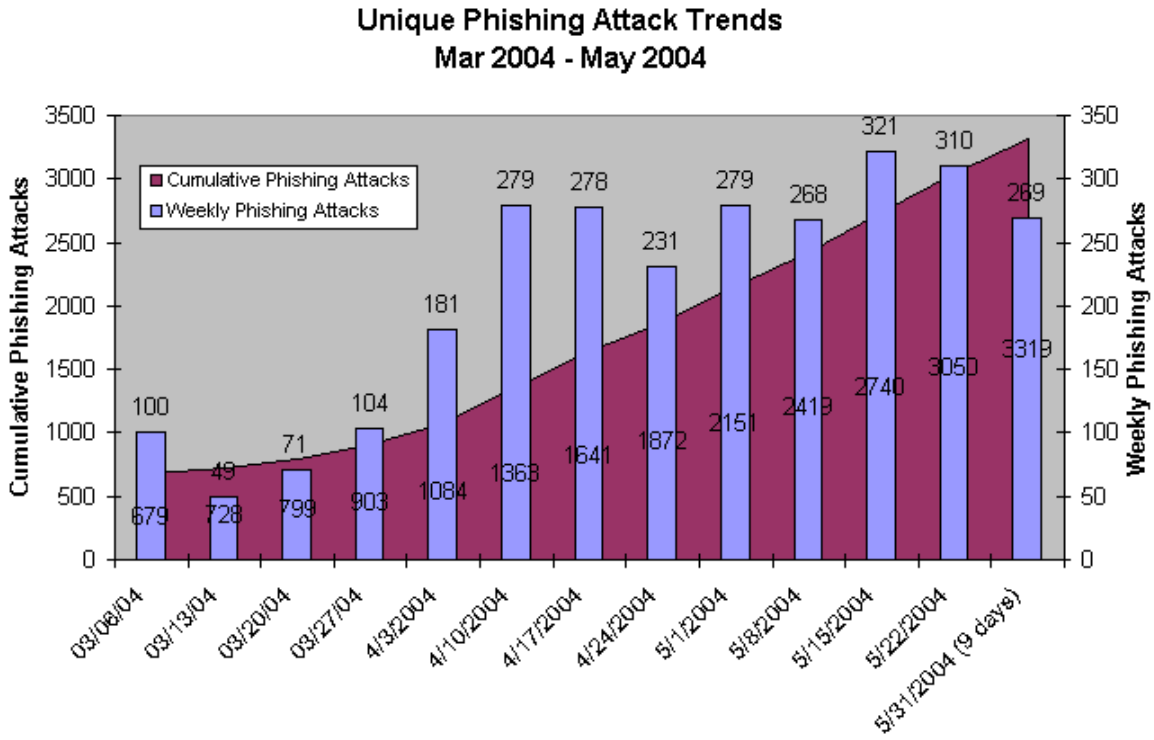
Phishing Attack Trends Report May, 2004

Phishing attacks use spoofed e-mails and fraudulent websites designed to fool recipients 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 up to 5% of recipients to respond to them. The result of these scams is that consumers suffer credit card fraud, identity theft, and financial loss.

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 May: **1197**
- Peak number of unique phishing attacks per week reported in May: **321**
- Organization most targeted by phishing attacks in May: **Citibank (370)**
- Business sector most targeted by phishing attacks in May: **Financial Services**
- Percentage of phishing attacks using spoofed email addresses: **95%**



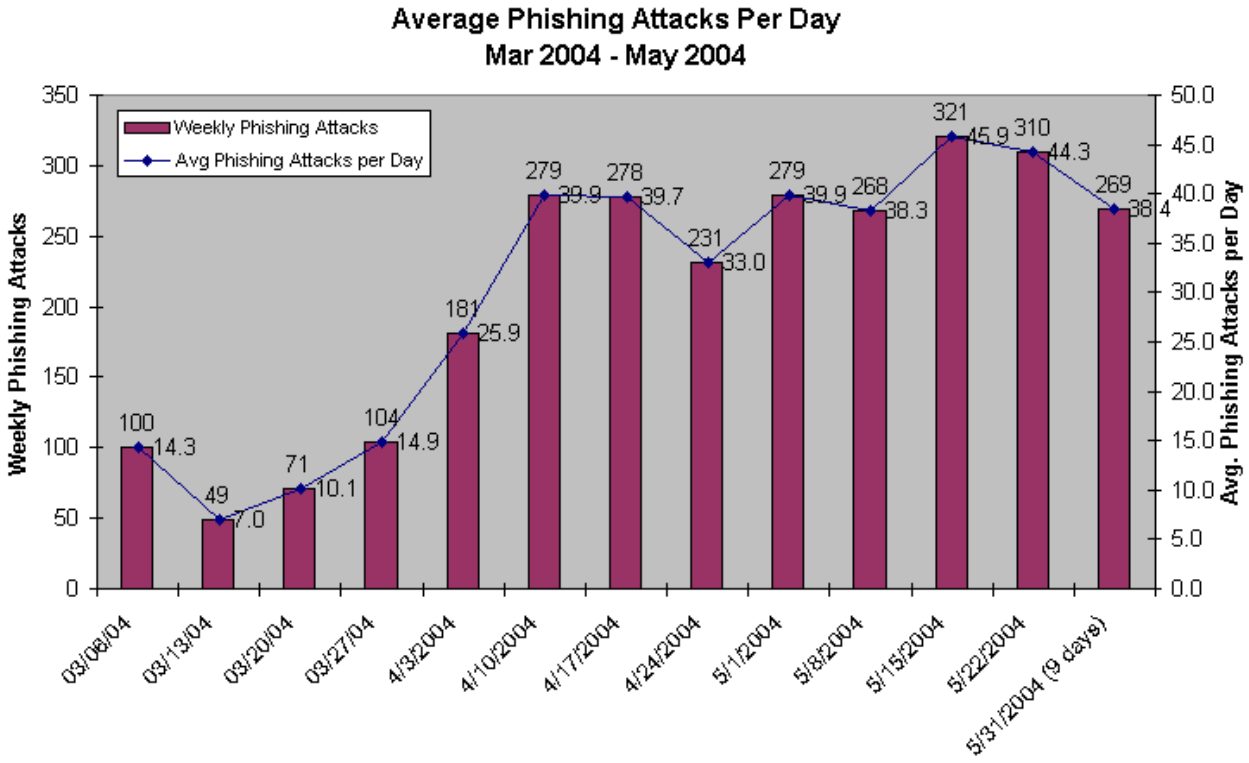
The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact Dan Maier at dmaier@antiphishing.org 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

In May, there were 1197 new, unique phishing attacks reported to the Anti-Phishing Working Group. This was a relatively minor 6% increase over the number of attacks reported in April (1125). The average number of phishing attacks per day in May was 38.6 (up slightly from the 37.5 per day for April). Analyzing this information on a weekly basis shows two weeks that averaged over 300 attacks, but a significant dip during the week of May 29. This may be due to the Labor Day holiday in the U.S., and a resultant reduction in reported phishing attacks.



Who Is Being Targeted By Phishing Attacks?

Most-Targeted Companies

In May, Citibank was (once again) the company whose brand was hijacked most often by phishers, although this represents a significant 22% drop in volume from the previous month.

eBay continues to be the target of a large and growing volume of phishing attacks (as does Paypal, which ended up in fourth place this month).

U.S. Bank was the third-most attacked brand in May, with a 170% surge in phishing attacks.

Other notable targets included Visa, with over 20 phishing attacks spoofing its brand, and AOL, which saw a doubling of phishing attacks.

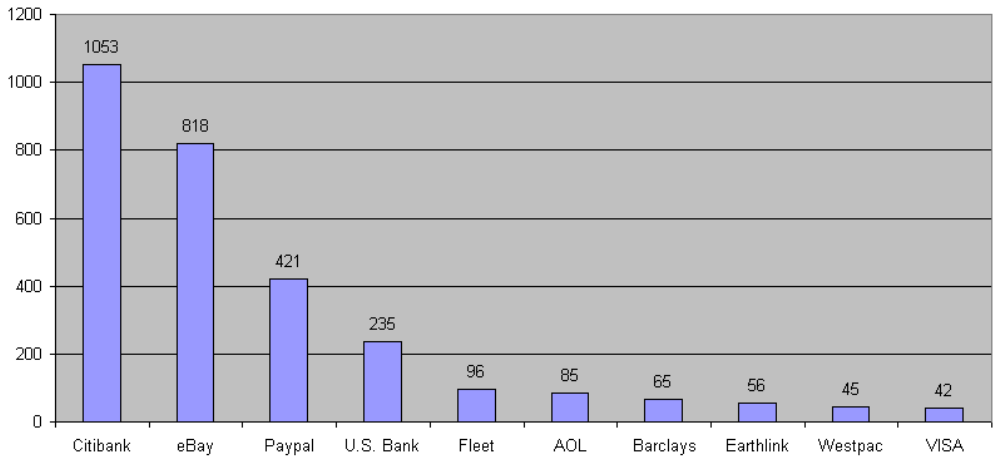
Unique Phishing Attacks by Targeted Company

Phish Target	May-04	Apr-04	Mar-04	Feb-04	Jan-04	Dec-03
Citibank	370	475	98	58	34	17
eBay	293	221	110	104	51	33
U.S. Bank	167	62	4	0	2	0
Paypal	149	135	63	42	10	16
Fleet	33	28	23	9	2	1
VISA	21	0	7	8	2	4
AOL	17	9	10	10	35	4
LLoyds	17	15	4	0	1	1
Barclays	15	31	11	6	1	1
Westpac	12	17	10	0	3	1
Nationwide	10	0	0	0	0	0
Halifax	9	6	1	0	1	0
Bank One	6	4	5	0	0	1
Chase	6	3	2	0	0	0
Earthlink	6	18	5	8	9	6
ANZ	4	7	4	0	0	3
Natwest	4	6	2	0	0	1
e-gold	3	5	2	2	0	2
HSBC	3	3	4	0	1	0
MSN	3	0	0	0	0	0
National Wes	3	0	0	0	0	0
Woolwich	3	0	0	0	0	0
Yahoo	3	2	3	4	2	0

Anti-Phishing Working Group

Over the past 7 months that phishing attacks have been reported to the APWG, its clear that phishers have focused their efforts on Citibank, eBay and Paypal.

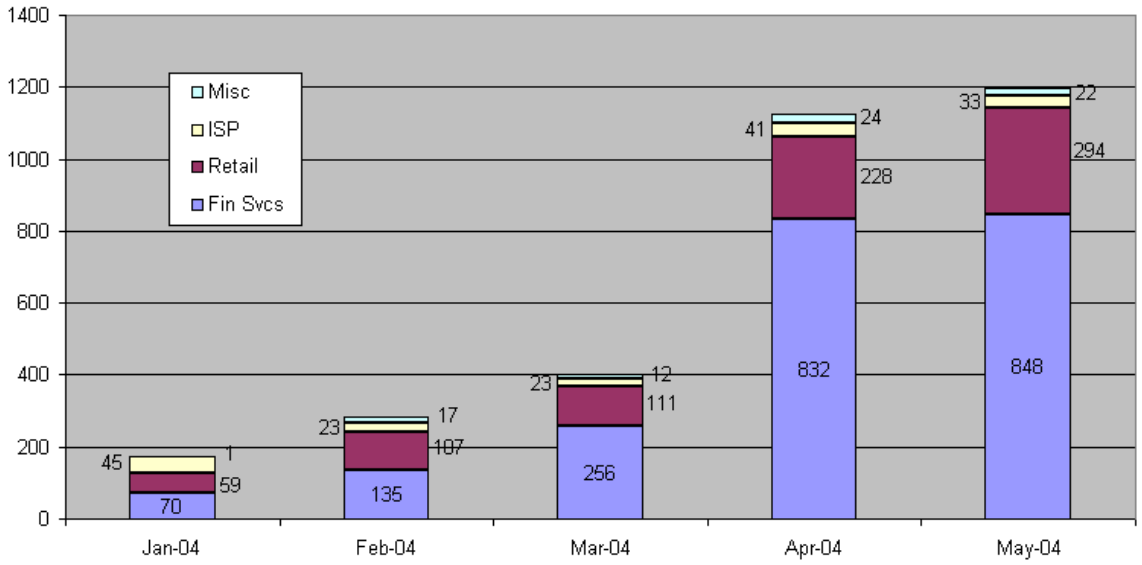
Cumulative Reported Phishing Attacks
Nov 03 - May 04



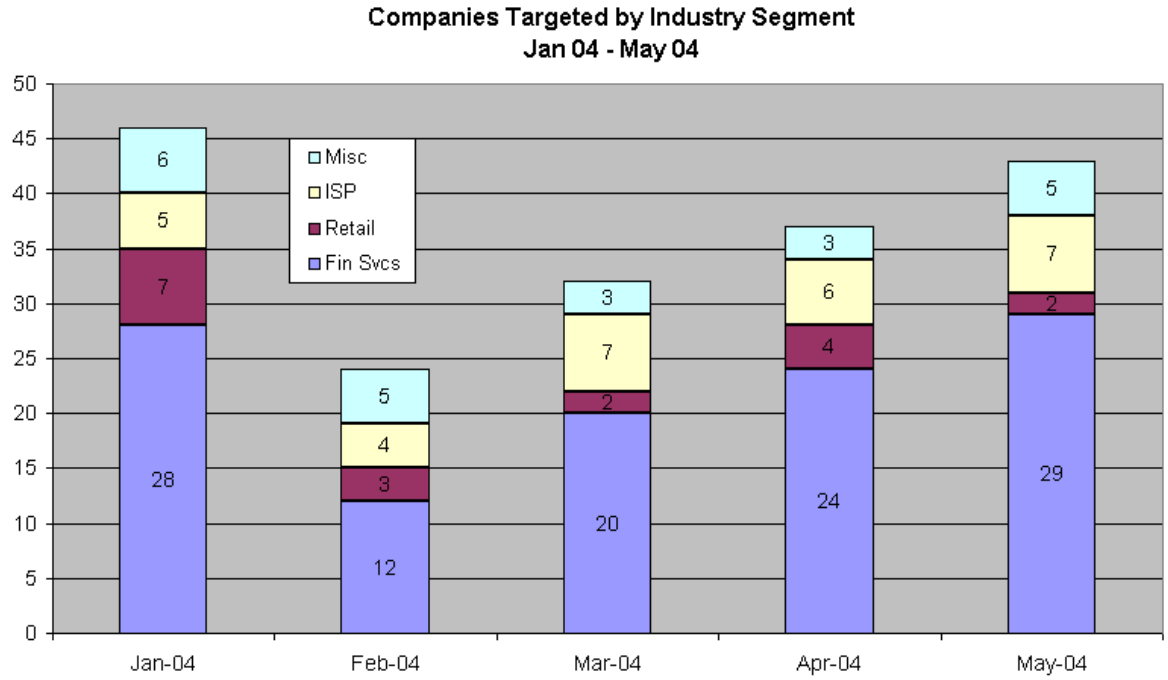
Most-Targeted Industry Sectors

Financial Services remains the most highly targeted industry sector by phishing attacks, both in terms of overall number of attacks, as well as number of companies targeted by phishers. The Retail sector (primarily driven by eBay) continues to follow as the next most-attractive industry segment for phishing.

Unique Phishing Attacks by Industry Segment
Jan 04 - May 04



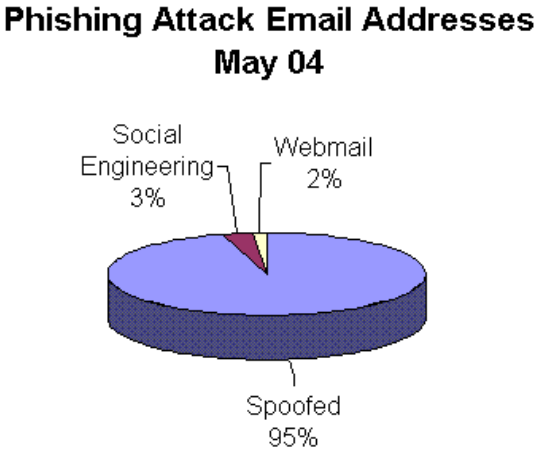
Anti-Phishing Working Group



EMAIL SOURCE ANALYSIS

95% of Phishing Attacks Use Spoofed Email Addresses

In analyzing the "From" address used by phishers for May attacks, we found that at least 95% of them were 'spoofed', or forged. In addition, only a very small percentage of phishing emails actually use "social engineering" email addresses or non-disguised Webmail addresses.



"Social engineering" email addresses use authentic Internet email domains that look similar to email addresses used by the companies they are spoofing. For example, one email address used to spoof Visa was "support@verify-visa.org". Note that this is NOT a valid email address for Visa, but is used to try to fool recipients via 'social engineering' into disclosing their credit card information. It is likely that some percentage of the social engineering and Webmail email addresses may also be forged, so the actual percentage of spoofed phishing emails is likely higher than 95%.

Anti-Phishing Working Group

The table below contains example email addresses from each of the three email source classifications we used to analyze the phishing attacks. Note that this analysis used about 80% of the phishing attacks submitted to the APWG – the rest were not usable for this analysis because they lacked sufficient header information to analyze the email source:

Spoofed Addresses	Social Engineering Addresses	Webmail Addresses
billing@aol.com	aol@billing.com	%MFROM@msn.com
AOLBilling@aol.com	update-account@american-on-line.com	mathieu@compuserve.com
services@aba.com	citicard@citigrop.com	w-e-account@aol.com
support@anz.com	support@earthlink-verified.com	vnqtsgzj-chyd@mail.com
customerservice@att.com	support@verified-earthlink.net	dxthncxr-tlwo@lycos.com
Domain@bankone.com	support@eBay.billing.com	zzyxslxs-qtgs@yahoo.com
support@barclays.com	ebay@aw-confirm.com	uqoeyuwl-invi@yahoo.de
users-billing39@barclays.co.uk	information@ebay-validation.info	abcii@earthlink.net
chasecreditcards@email.chase.com	billing@ebay.staff.com	shadowvamp04@yahoo.com.au
support@citibank.com	directmail@yahoo-inc.com	
suspend@ebay.com	support@lloydstsd.co.uk	
aw-confirmation@ebay.com	mso@paypalsecure.com	
customers@experian.com	support@visa-verify.net	
service@fleet.com	support@verify-visa.net	
users-billing42@halifax.co.uk	support@verify-visa.org	
users-billing32@lloydstsb.co.uk	support@verify-visa.info	
support@msn.com	wachovia@wachoviaemail.com	

Anti-Phishing Working Group
APWG
www.antiphishing.org

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 currently over 200 member organizations participating in the APWG. 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.