Anti-Phishing Working Group

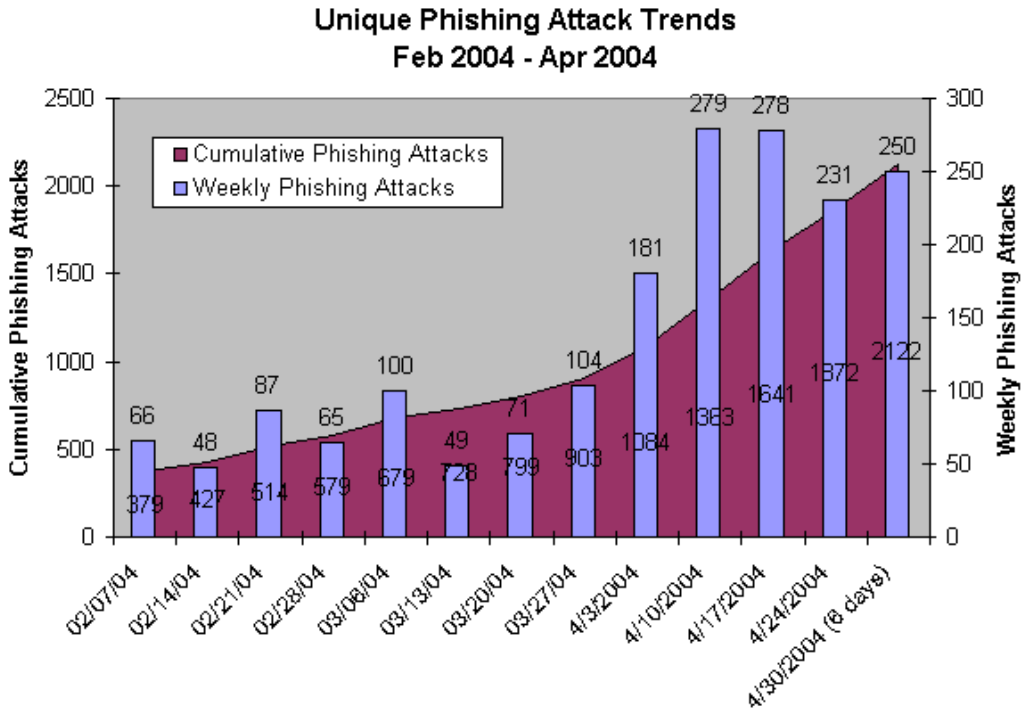
Phishing Attack Trends Report April, 2004

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 April: **1125**
- Average number of unique phishing attacks per day reported in April: **37.5**
- Organization most targeted by phishing attacks in April: **Citibank, 475 attacks**
- Business sector most targeted by phishing attacks in April: **Financial Services**



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.

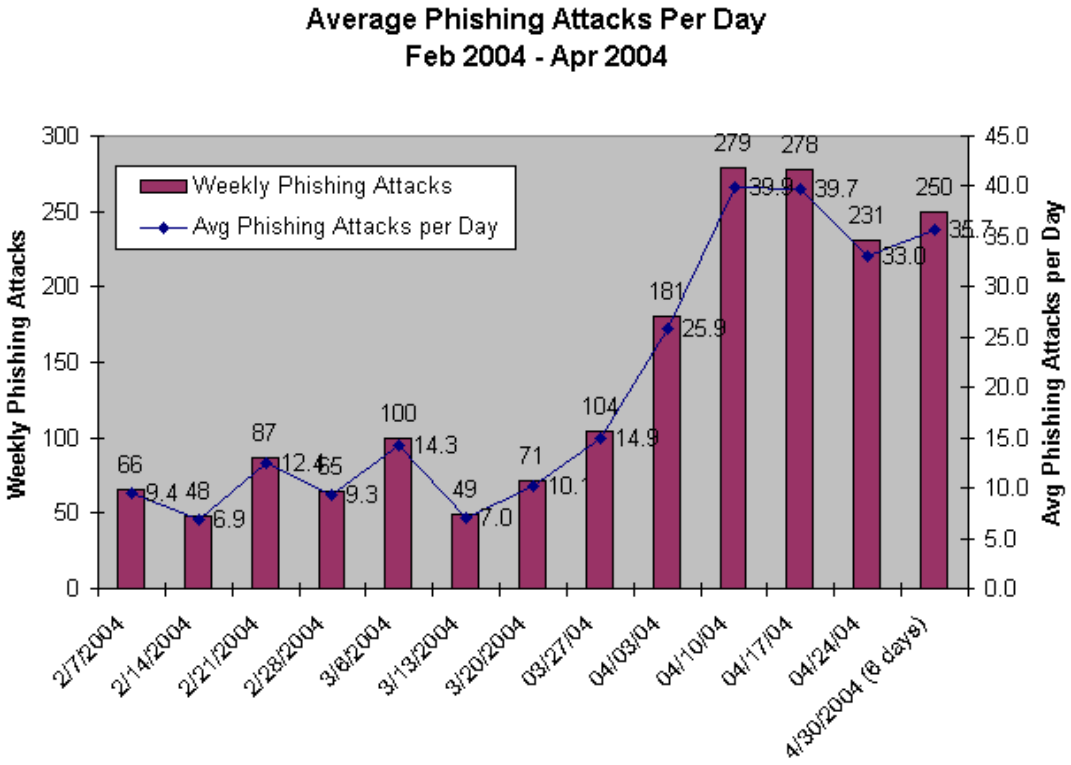
Analysis for the **Phishing Attack Trends Report** has been donated by the Tumbleweed Communications Message Protection Lab. The mission of the Tumbleweed Message Protection Lab is to analyze enterprise email threats (e.g. spam, email fraud, viruses, etc) and design new email protection technologies.

TUMBLEWEED COMMUNICATIONS

Anti-Phishing Working Group

Email Phishing Attack Trends

In April, there were 1125 new, unique phishing attacks reported to the Anti-Phishing Working Group. This was a 180% increase over the number of attacks reported in March (402). The average number of phishing attacks per day grew significantly in April to 37.5 (from 13.0 in March). Analyzing this information on a weekly basis shows two weeks that averaged almost 40 attacks per day, and weekly volumes consistently over 200 attacks per week. This marks a huge increase in the volume of phishing attacks.



Who Is Being Targeted By Phishing Attacks?

Most-Targeted Companies

In April, Citibank was barraged by an average of almost 16 phishing attacks per day. The 475 attacks targeted at Citibank, representing a 385% increase from March, exceeded the total attacks reported against all organizations for the prior month (402).

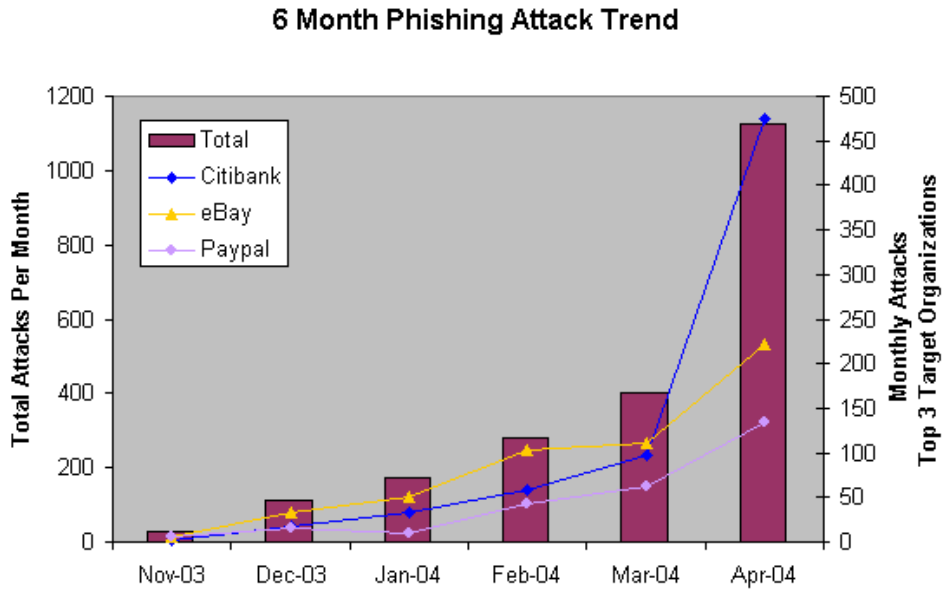
eBay and Paypal were the second and third most targeted companies respectively, with the volume of attacks against each of these organizations doubling from the prior month.

It is noteworthy that 15 of the top 20 targeted organizations are financial services organizations, with 3 ISPs and 2 'others' rounding out the mix.

Unique Phishing Attacks by Targeted Company

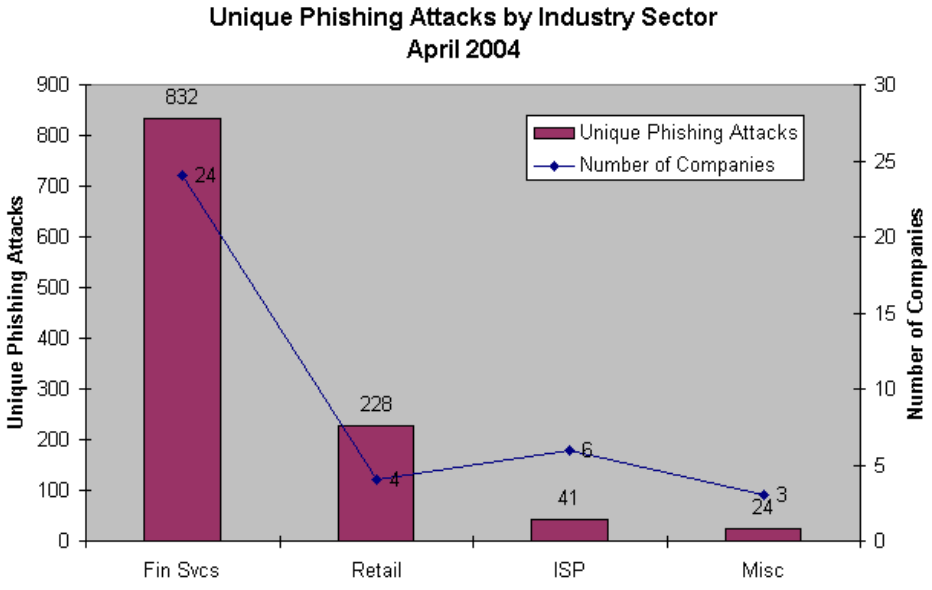
Phish Target	Apr-04	Mar-04	Feb-04	Jan-04	Dec-03	Nov-03
Citibank	475	98	58	34	17	1
eBay	221	110	104	51	33	6
Paypal	135	63	42	10	16	6
US Bank	62	4	0	2	0	0
Barclays	31	11	6	1	1	0
Fleet Bank	28	23	9	2	1	0
Earthlink	18	5	8	9	6	4
Westpac	17	10	0	3	1	2
Lloyds	15	4	0	1	1	0
AOL	9	10	10	35	4	0
SBC	9	1	0	0	0	0
ANZ	7	4	0	0	3	0
FDIC	7	0	2	2	0	0
Halifax	6	1	0	1	0	0
National Bank	6	0	0	0	0	0
NatWest	6	2	0	0	1	0
E-Gold	5	2	2	0	2	0
Suntrust Bank	5	1	0	0	0	0
Bank One	4	5	0	0	1	0
Microsoft	4	5	1	6	0	0

With 6 months of data available for analysis, it is interesting to look at the trends for overall phishing attacks, as well as the top 3 targeted companies. Overall, unique phishing attacks reported to the APWG have been growing at 110% *per month*, from 28 originally reported in November 2003 to 1125 reported in April 2004. This represents a 40X growth over the past six months, or almost 4000%. And it is quite clear that Citibank, eBay and Paypal are favorite targets of phishers – attacks against these organizations have shown a *monthly* growth rate of 250%, 105%, and 85% respectively.



Most-Targeted Industry Sectors

The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total attacks as well as number of companies targeted. The Retail sector (primarily eBay) continues to follow, although there are significantly fewer retailers targeted. The Financial Services sector averaged almost 35 reported phishing attacks per company in April, although this number is significantly skewed by Citibank receiving 475 of the attacks.

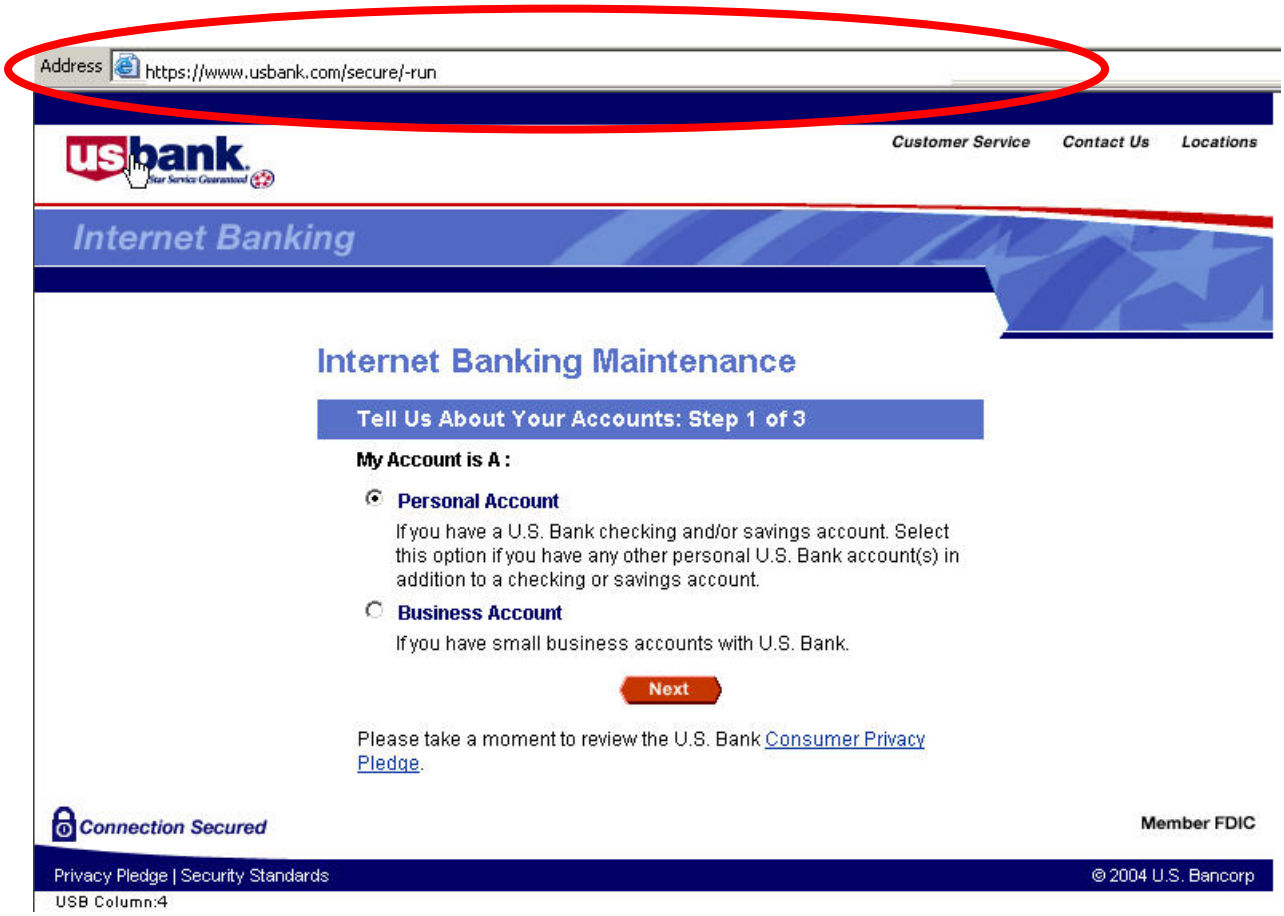


Anti-Phishing Working Group

APWG THREAT ADVISORY ALERT

Browser Web Address Spoofed Using 'Floating' Window

In a new twist on a recently identified phishing attack technique, phishers are putting 'floating' windows over the Address Bar in a Web browser to fool people into thinking they are on a legitimate site. It works like this: once the link to the phisher's site is clicked, a perfectly branded Web page is opened. But to complete the scam, the phisher needs to disguise the Web address so that the victim will be fooled into thinking he/she is on a legitimate site. To do this, the phisher has developed some Javascript that draws a window showing a "legitimate" address above the victim's Internet Explorer Web Address bar (see below).



Upon closer inspection of the Web Address bar (see below), it is clear that this 'replacement' is not perfect – it overlaps the address bar frame slightly. Unfortunately, it is quite adequate to fool most people who tend to see what they expect on a cursory glance at the Web Address bar. Also note that, although the address bar is covered, the status bar remains correct. When clicking 'next' on the first page, one could notice the 'loading http://validation-required.info/...' message in the status bar.

After the victim clicks 'next' on the first page, the second phish page loads. It is here that the phish demands the personal information from the victim.

Anti-Phishing Working Group

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.