The Anti-Phishing Working Group

- Industry association focused on eliminating identity theft and fraud from the growing problem of phishing and email spoofing
- Founded in 2003 by Tumbleweed Communications, Financial Institutions, ISPs, Law Enforcement Organisations and Technology Providers
- First meeting November 2003
- Now over 250 member organisations
- www.antiphishing.org
- Report phishing to reportphishing@antiphishing.org
**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.
First known attacks on AOL accounts in 1996

Sporadic attacks up until 2003, mainly AOL, eBay and PayPal

Major growth from mid-2003 until present day
  - Focus on English language – U.S.A, Australia and U.K.

2004 – first non-English language attacks on Swiss Banks

Increasing sophistication of attacks
The Growth of Phishing

Unique Phishing Attacks (to end May 2004)
## Phishing Targets (May)

<table>
<thead>
<tr>
<th></th>
<th>May-04</th>
<th>Apr-04</th>
<th>Mar-04</th>
<th>Feb-04</th>
<th>Jan-04</th>
<th>Dec-03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citibank</td>
<td>370</td>
<td>475</td>
<td>98</td>
<td>58</td>
<td>34</td>
<td>17</td>
</tr>
<tr>
<td>eBay</td>
<td>293</td>
<td>221</td>
<td>110</td>
<td>104</td>
<td>51</td>
<td>33</td>
</tr>
<tr>
<td>U.S. Bank</td>
<td>167</td>
<td>62</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Paypal</td>
<td>149</td>
<td>135</td>
<td>63</td>
<td>42</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>Fleet</td>
<td>33</td>
<td>28</td>
<td>23</td>
<td>9</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Visa</td>
<td>21</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>AOL</td>
<td>17</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>35</td>
<td>4</td>
</tr>
<tr>
<td>Lloyds TSB</td>
<td>17</td>
<td>15</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Barclays</td>
<td>15</td>
<td>31</td>
<td>11</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Westpac</td>
<td>12</td>
<td>17</td>
<td>10</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Nationwide</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Halifax</td>
<td>9</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Natwest</td>
<td>7</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Bank One</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Chase</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Earthlink</td>
<td>6</td>
<td>18</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>ANZ</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>e-gold</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>HSBC</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>MSN</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Woolwich</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yahoo</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
Phishing Targets (to May 2004)
Typical Emails

Spoofed From Address

Faked and encoded URL
Typical Website

- Genuine Citibank site
- Popup Window on Phisher’s site
Attack trends

- **Email sources**
  - Majority relayed through compromised adsl/cable connected Windows machines
  - 95% of FROM: addresses spoofed
Attack trends

• **Websites**
  » Compromised Windows Cable/ADSL machines
    • Worms/trojans/backdoors
    • Open remote access services (VNC)

  » Subverted legitimate sites
    • Wide open/badly configured machines
    • Unpatched vulnerabilities

  » Throw away hosting
Key elements to phishing

• Email should not be traceable

• Web site should not be traceable

• Money should not be traceable

• User needs reason to give details:-
  » “your account will be deactivated…”
  » “fraud on your account…”
  » “win a prize…”

• Web site should look convincing:-
  » Correct colours/logos
  » Not given away by URL….
Hiding the URL

- Sub-domain looks like bank
- Legitimate unrelated domain
Hiding the URL
Hiding the URL: Pop up name window
Hiding the URL: Pop up on top

Genuine Citibank site

Popup Window on Phisher’s site
Hiding the URL: Fake browser parts

- Fake browser address bar
- Fake padlock
Approaches to Countering Phishing

- **Legislation**
  - It’s already illegal!

- **Spam filters**
  - Can catch a proportion
  - Relies on continual updates
  - Needs action from recipients/ISPs

- **Education**
  - Tell people about phishing
  - Educate people about security vulnerabilities

- **Two Factor Web Authentication**
  - Cost of roll out

- **Email authentication**
  - Solves the underlying problem – spoofing of FROM addresses
    - Sender-ID/Caller-ID/SPF
    - S/MIME digital signatures
  - Will take time to roll out