

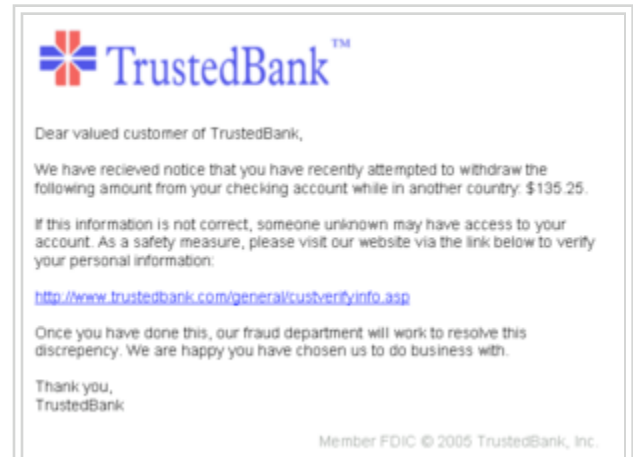
Phishing

From Wikipedia, the free encyclopedia

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging,^[1] and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users,^[2] and exploits the poor usability of current web security technologies.^[3] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of *fishing*,^[4] probably influenced by *phreaking*,^[5] ^[6] and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen.



An example of a phishing e-mail, disguised as an official e-mail from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the *phisher's* website. Note the misspelling of the words *received* and *discrepancy*. Also note that although the URL of the bank's webpage appears to be legitimate, the hyperlink would actually be pointed at the phisher's webpage.

History and current status of phishing

A phishing technique was described in detail, in a paper and presentation delivered to the International HP Users Group, Interex.^[7] The first recorded mention of the term "phishing" is on the alt.online-service.america-online Usenet newsgroup on January 2, 1996,^[8] although the term may have appeared earlier in the print edition of the hacker magazine *2600*.^[9]

A recent and popular case of phishing is the suspected Chinese phishing campaign targeting Gmail accounts of highly ranked officials of the United States and South Korean's Government, military, and Chinese political activists.^[10] The Chinese government continues to deny accusations of taking part in cyber-attacks from within its borders, but evidence has been revealed that China's own People's Liberation Army has assisted in the coding of cyber-attack software.^[11]

Early phishing on AOL

Phishing on AOL was closely associated with the warez community that exchanged pirated software and the hacking scene that perpetrated credit card fraud and other online crimes. After AOL brought in measures in late 1995 to prevent using fake, algorithmically generated credit card numbers to open accounts, AOL crackers resorted to phishing for legitimate accounts^[12] and exploiting AOL.

A phisher might pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal his password.^[13] In order to lure the victim into giving up sensitive information the

message might include imperatives like "**verify your account**" or "**confirm billing information**". Once the victim had revealed the password, the attacker could access and use the victim's account for fraudulent purposes or spamming. Both phishing and warezing on AOL generally required custom-written programs, such as AOHell. Phishing became so prevalent on AOL that they added a line on all instant messages stating: "no one working at AOL will ask for your password or billing information", though even this didn't prevent some people from giving away their passwords and personal information if they read and believed the IM first. A user using both an AIM account and an AOL account from an ISP simultaneously could phish AOL members with relative impunity as internet AIM accounts could be used by non-AOL internet members and could not be actioned (i.e.- reported to AOL TOS department for disciplinary action.)

Eventually, AOL's policy enforcement with respect to phishing and warez became stricter and forced pirated software off AOL servers. AOL simultaneously developed a system to promptly deactivate accounts involved in phishing, often before the victims could respond. The shutting down of the warez scene on AOL caused most phishers to leave the service.^[14]

Transition from AOL to financial institutions

The capture of AOL account information may have led phishers to misuse credit card information, and to the realization that attacks against online payment systems were feasible. The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-9/11 id check" shortly after the September 11 attacks on the World Trade Center.^[15] Both were viewed at the time as failures, but can now be seen as early experiments towards more fruitful attacks against mainstream banks. By 2004, phishing was recognized as a fully industrialized part of the economy of crime: specializations emerged on a global scale that provided components for cash, which were assembled into finished attacks.^{[16][17]}

Phishing techniques

Recent phishing attempts

Phishers are targeting the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers.^[18] While the first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phishers may in principle be able to determine which banks potential victims use, and target bogus e-mails accordingly.^[19] Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft;^[20] in late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details.^[21] Experiments show a success rate of over 70% for phishing attacks on



A chart showing the increase in phishing reports from October 2004 to June 2005.

social networks.^[22]

The RapidShare file sharing site has been targeted by phishing to obtain a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cooldown times between uploads.^[23]

Attackers who broke into TD Ameritrade's database (containing all 6.3 million customers' social security numbers, account numbers and email addresses as well as their names, addresses, dates of birth, phone numbers and trading activity) also wanted the account usernames and passwords, so they launched a follow-up spear phishing attack.^[24]

Almost half of phishing thefts in 2006 were committed by groups operating through the *Russian Business Network* based in St. Petersburg.^[25]

There are anti-phishing websites which publish exact messages that have been recently circulating the internet, such as FraudWatch International and Millersmiles. Such sites often provide specific details about the particular messages.^{[26][27]} Nowadays to reduce working with the source code of web pages, Hackers have implemented a phishing tool called **Super Phisher** that makes the work easy when compared to manual method of creating a phishing websites.

List of phishing techniques

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spear Phishing

Targeted versions of phishing have been termed **spearphishing**.^[28]

Clone Phishing

A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a re-send of the original or an updated version to the original.

This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high

profile targets within businesses, and the term **whaling** has been coined for these kinds of attacks.^[29]

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example URL, `http://www.yourbank.example.com/`, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually this URL points to the "*yourbank*" (i.e. phishing) section of the *example* website. Another common trick is to make the displayed text for a link (the text between the `<A>` tags) suggest a reliable destination, when the link actually goes to the phishers' site. The following example link, `//en.wikipedia.org/wiki/Genuine`, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them.^[30] Hovering your cursor over the link for a couple of seconds *may* do a similar thing, but this can still be set by the phisher.

A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing^[31] or homograph attack,^[32] phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain.^{[33][34][35]} Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website.

Filter evasion

Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.^[36]

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar.^[37] This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.^[38]

An attacker can even use flaws in a trusted website's own scripts against the victim.^[39] These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.^[40]

A Universal Man-in-the-middle (MITM) Phishing Kit, discovered in 2007, provides a simple-to-use

interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.^[41]

To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites. These look much like the real website, but hide the text in a multimedia object.^[42]

Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.^[43] Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.^[44]

Other techniques

- Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information.^[45]
- One of the latest phishing techniques is tabnabbing. It takes advantage of the multiple tabs that users use and silently redirects a user to the affected site.
- Evil twins is a phishing technique that is hard to detect. A phisher creates a fake wireless network that looks similar to a legitimate public network that may be found in public places such as airports, hotels or coffee shops. Whenever someone logs on to the bogus network, fraudsters try to capture their passwords and/or credit card information.

Damage caused by phishing

The damage caused by phishing ranges from denial of access to e-mail to substantial financial loss. It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US\$929 million. United States businesses lose an estimated US\$2 billion per year as their clients become victims.^[46] In 2007, phishing attacks escalated. 3.6 million adults lost US\$3.2 billion in the 12 months ending in August 2007.^[47] Microsoft claims these estimates are grossly exaggerated and puts the annual phishing loss in the US at US\$60 million.^[48] In the United Kingdom losses from web banking fraud—mostly from phishing—almost doubled to GB£23.2m in 2005, from GB£12.2m in 2004,^[49] while 1 in 20 computer users claimed to have lost out to phishing in 2005.^[50]

The stance adopted by the UK banking body APACS is that "customers must also take sensible precautions ... so that they are not vulnerable to the criminal."^[51] Similarly, when the first spate of phishing attacks hit the Irish Republic's banking sector in September 2006, the Bank of Ireland initially refused to cover losses suffered by its customers (and it still insists that its policy is not to do so^[52]),

although losses to the tune of €11,300 were made good.^[53]

Anti-phishing

There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing. Most new internet browsers come with anti-phishing software.

Social responses

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback.^[54] One newer phishing tactic, which uses phishing e-mails targeted at a specific company, known as *spear phishing*, has been harnessed to train individuals at various locations, including United States Military Academy at West Point, NY. In a June 2004 experiment with spear phishing, 80% of 500 West Point cadets who were sent a fake e-mail from a non-existent Col. Robert Melville at West Point, were tricked into clicking on a link that would supposedly take them to a page where they would enter personal information. (The page informed them that they had been lured.)^[55]

People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the e-mail apparently originates to check that the e-mail is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message.^[56]

Nearly all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to phishers. Some companies, for example PayPal, always address their customers by their username in e-mails, so if an e-mail addresses the recipient in a generic fashion ("*Dear PayPal customer*") it is likely to be an attempt at phishing.^[57] E-mails from banks and credit card companies often include partial account numbers. However, recent research^[58] has shown that the public do not typically distinguish between the first few digits and the last few digits of an account number—a significant problem since the first few digits are often the same for all clients of a financial institution. People can be trained to have their suspicion aroused if the message does not contain any specific personal information. Phishing attempts in early 2006, however, used personalized information, which makes it unsafe to assume that the presence of personal information alone guarantees that a message is legitimate.^[59] Furthermore, another recent study concluded in part that the presence of personal information does not significantly affect the success rate of phishing attacks,^[60] which suggests that most people do not pay attention to such details.

The Anti-Phishing Working Group, an industry and law enforcement association, has suggested that conventional phishing techniques could become obsolete in the future as people are increasingly aware of the social engineering techniques used by phishers.^[61] They predict that pharming and other uses of malware will become more common tools for stealing information.

Everyone can help educate the public by encouraging safe practices, and by avoiding dangerous ones. Unfortunately, even well-known players are known to incite users to hazardous behaviour, e.g. by requesting their users to reveal their passwords for third party services, such as email.^[62]

Technical responses

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

Helping to identify legitimate websites

Most websites targeted for phishing are secure websites meaning that SSL with strong PKI cryptography is used for server authentication, where the website's URL is used as identifier. In theory it should be possible for the SSL authentication to be used to confirm the site to the user, and this was SSL v2's design requirement and the meta of secure browsing. But in practice, this is easy to trick.

The superficial flaw is that the browser's security user interface (UI) is insufficient to deal with today's strong threats. There are three parts to secure authentication using TLS and certificates: indicating that the connection is in authenticated mode, indicating which site the user is connected to, and indicating which authority says it is this site. All three are necessary for authentication, and need to be confirmed by/to the user.

Secure connection

The standard display for secure browsing from the mid-1990s to mid-2000s was the padlock. In 2005, Mozilla fielded a yellow address bar as a better indication of the secure connection. This innovation was later reversed due to the EV certificates, which replaced certain certificates providing a high level of organization identity verification with a green display, and other certificates with an extended blue favicon box to the left of the URL bar (in addition to the switch from "http" to "https" in the url itself).

Which site

The user is expected to confirm that the domain name in the browser's URL bar was in fact where they intended to go. URLs can be too complex to be easily parsed. Users often do not know or recognise the URL of the legitimate sites they intend to connect to, so that the authentication becomes meaningless.^[3] A condition for meaningful server authentication is to have a server identifier that is meaningful to the user; many ecommerce sites will change the domain names within their overall set of websites, adding to the opportunity for confusion. Simply displaying the domain name for the visited website^[63], as some anti-phishing toolbars do, is not sufficient.

Some newer browsers, such as Internet Explorer 8, display the entire URL in grey, with just the domain name itself in black, as a means of assisting users in identifying fraudulent URLs.

An alternate approach is the petname extension for Firefox which lets users type in their own labels for

websites, so they can later recognize when they have returned to the site. If the site is not recognised, then the software may either warn the user or block the site outright. This represents user-centric identity management of server identities.^[64] Some suggest that a graphical image selected by the user is better than a petname.^[65]

With the advent of EV certificates, browsers now typically display the organisation's name in green, which is much more visible and is hopefully more consistent with the user's expectations. Browser vendors have chosen to limit this prominent display only to EV certificates, leaving the user to fend for himself with all other certificates.

Who is the Authority

The browser needs to state who the authority is that makes the claim of who the user is connected to. At the simplest level, no authority is stated, and therefore the browser is the authority, as far as the user is concerned. The browser vendors take on this responsibility by controlling a *root list* of acceptable CAs. This is the current standard practice.

The problem with this is that not all certification authorities (CAs) employ equally good nor applicable checking, regardless of attempts by browser vendors to control the quality. Nor do all CAs subscribe to the same model and concept that certificates are only about authenticating ecommerce organisations. *Certificate Manufacturing* is the name given to low-value certificates that are delivered on a credit card and an email confirmation; both of these are easily perverted by fraudsters.^[citation needed] Hence, a high-value site may be easily spoofed by a valid certificate provided by another CA. This could be because the CA is in another part of the world, and is unfamiliar with high-value ecommerce sites, or it could be that no care is taken at all. As the CA is only charged with protecting its own customers, and not the customers of other CAs, this flaw is inherent in the model.

The solution to this is that the browser should show, and the user should be familiar with, the name of the authority. This presents the CA as a brand, and allows the user to learn the handful of CAs that she is likely to come into contact within her country and her sector. The use of brand is also critical to providing the CA with an incentive to improve their checking, as the user will learn the brand and demand good checking for high-value sites.

This solution was first put into practice in early IE7 versions, when displaying EV certificates.^[66] In that display, the issuing CA is displayed. This was an isolated case, however. There is resistance to CAs being branded on the chrome, resulting in a fallback to the simplest level above: the browser is the user's authority.^[citation needed]

Fundamental flaws in the security model of secure browsing

Experiments to improve the security UI have resulted in benefits, but have also exposed fundamental flaws in the security model. The underlying causes for the failure of the SSL authentication to be employed properly in secure browsing are many and intertwined.

Users tend not to check security information, even when it is explicitly displayed to them. For example,

the vast majority of warnings for sites are for misconfigurations, not a MITM (man in the middle attack). Users have learned to bypass the warnings and treat all warnings with the same disdain, resulting in Click-through syndrome. For example, Firefox 3 has a 4-click process for adding an exception, but it has been shown to be ignored by an experienced user in a real case of MITM.

Another underlying factor is the lack of support for virtual hosting. The specific causes are a lack of support for Server Name Indication in TLS webserver, and the expense and inconvenience of acquiring certificates. The result is that the use of authentication is too rare to be anything but a special case. This has caused a general lack of knowledge and resources in authentication within TLS, which in turn has meant that the attempts by browser vendors to upgrade their security UIs have been slow and lackluster.

The security model for secure browser includes many participants: user, browser vendor, developers, CA, auditor, webserver vendor, ecommerce site, regulators (e.g., FDIC), and security standards committees. There is a lack of communication between different groups that are committed to the security model. E.g., although the understanding of authentication is strong at the protocol level of the IETF committees, this message does not reach the UI groups. Webserver vendors do not prioritize the Server Name Indication (TLS/SNI) fix, not seeing it as a security fix but instead a new feature. In practice, all participants look to the others as the source of the failures leading to phishing, hence the local fixes are not prioritized.

Matters improved slightly with the CAB Forum, as that group includes browser vendors, auditors and CAs.^[*citation needed*] But the group did not start out in an open fashion, and the result suffered from commercial interests of the first players, as well as a lack of parity between the participants.^[*citation needed*] Even today, CAB forum is not open, and does not include representation from small CAs, end-users, ecommerce owners, etc.^[*citation needed*]

Vendors commit to standards, which results in an outsourcing effect when it comes to security. Although there have been many and good experiments in improving the security UI, these have not been adopted because they are not standard, or clash with the standards. Threat models can re-invent themselves in around a month; Security standards take around 10 years to adjust.^[*citation needed*]

Control mechanisms employed by the browser vendors over the CAs have not been substantially updated; the threat model has.^[*citation needed*] The control and quality process over CAs is insufficiently tuned to the protection of users and the addressing of actual and current threats.^[*citation needed*] Audit processes are in great need of updating.^[*citation needed*] The recent EV Guidelines documented the current model in greater detail, and established a good benchmark, but did not push for any substantial changes to be made.^[*citation needed*]

Browsers alerting users to fraudulent websites

Another popular approach to fighting phishing is to maintain a list of known phishing sites and to check websites against the list. Microsoft's IE7 browser, Mozilla Firefox 2.0, Safari 3.2, and Opera all contain this type of anti-phishing measure.^{[67][68][69][70]} Firefox 2 used Google anti-phishing software. Opera 9.1 uses live blacklists from PhishTank and GeoTrust, as well as live whitelists from GeoTrust. Some

implementations of this approach send the visited URLs to a central service to be checked, which has raised concerns about privacy.^[71] According to a report by Mozilla in late 2006, Firefox 2 was found to be more effective than Internet Explorer 7 at detecting fraudulent sites in a study by an independent software testing company.^[72]

An approach introduced in mid-2006 involves switching to a special DNS service that filters out known phishing domains: this will work with any browser,^[73] and is similar in principle to using a hosts file to block web adverts.

To mitigate the problem of phishing sites impersonating a victim site by embedding its images (such as logos), several site owners have altered the images to send a message to the visitor that a site may be fraudulent. The image may be moved to a new filename and the original permanently replaced, or a server can detect that the image was not requested as part of normal browsing, and instead send a warning image.^{[74][75]}

Augmenting password logins

The Bank of America's website^{[76][77]} is one of several that ask users to select a personal image, and display this user-selected image with any forms that request a password. Users of the bank's online services are instructed to enter a password only when they see the image they selected. However, a recent study suggests few users refrain from entering their password when images are absent.^{[78][79]} In addition, this feature (like other forms of two-factor authentication) is susceptible to other attacks, such as those suffered by Scandinavian bank Nordea in late 2005,^[80] and Citibank in 2006.^[81]

A similar system, in which an automatically generated "Identity Cue" consisting of a colored word within a colored box is displayed to each website user, is in use at other financial institutions.^[82]

Security skins^{[83][84]} are a related technique that involves overlaying a user-selected image onto the login form as a visual cue that the form is legitimate. Unlike the website-based image schemes, however, the image itself is shared only between the user and the browser, and not between the user and the website. The scheme also relies on a mutual authentication protocol, which makes it less vulnerable to attacks that affect user-only authentication schemes.

Still another technique relies on a dynamic grid of images that is different for each login attempt. The user must identify the pictures that fit their pre-chosen categories (such as dogs, cars and flowers). Only after they have correctly identified the pictures that fit their categories are they allowed to enter their alphanumeric password to complete the login. Unlike the static images used on the Bank of America website, a dynamic image-based authentication method creates a one-time passcode for the login, requires active participation from the user, and is very difficult for a phishing website to correctly replicate because it would need to display a different grid of randomly generated images that includes the user's secret categories.^[85]

Eliminating phishing mail

Specialized spam filters can reduce the number of phishing e-mails that reach their addressees' inboxes. These approaches rely on machine learning^[86] and natural language processing approaches to classify phishing e-mails.^{[87][88]}

Monitoring and takedown

Several companies offer banks and other organizations likely to suffer from phishing scams round-the-clock services to monitor, analyze and assist in shutting down phishing websites.^[89] Individuals can contribute by reporting phishing to both volunteer and industry groups,^[90] such as PhishTank.^[91] Individuals can also contribute by reporting phone phishing attempts to Phone Phishing,^[92] Federal Trade Commission.^[93]

Legal responses

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information.^[94] Other countries have followed this lead by tracing and arresting phishers. A phishing kingpin, Valdir Paulo de Almeida, was arrested in Brazil for leading one of the largest phishing crime rings, which in two years stole between US\$18 million and US\$37 million.^[95] UK authorities jailed two men in June 2005 for their role in a phishing scam,^[96] in a case connected to the U.S. Secret Service Operation Firewall, which targeted notorious "carder" websites.^[97] In 2006 eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo Japan Web sites, netting themselves ¥100 million (US\$870,000).^[98] The arrests continued in 2006 with the FBI Operation Cardkeeper detaining a gang of sixteen in the U.S. and Europe.^[99]

In the United States, Senator Patrick Leahy introduced the *Anti-Phishing Act of 2005* in Congress on March 1, 2005. This bill, if it had been enacted into law, would have subjected criminals who created fake web sites and sent bogus e-mails in order to defraud consumers to fines of up to US\$250,000 and prison terms of up to five years.^[100] The UK strengthened its legal arsenal against phishing with the Fraud Act 2006,^[101] which introduces a general offence of fraud that can carry up to a ten year prison sentence, and prohibits the development or possession of phishing kits with intent to commit fraud.^[102]

Companies have also joined the effort to crack down on phishing. On March 31, 2005, Microsoft filed 117 federal lawsuits in the U.S. District Court for the Western District of Washington. The lawsuits accuse "John Doe" defendants of obtaining passwords and confidential information. March 2005 also saw a partnership between Microsoft and the Australian government teaching law enforcement officials how to combat various cyber crimes, including phishing.^[103] Microsoft announced a planned further 100 lawsuits outside the U.S. in March 2006,^[104] followed by the commencement, as of November 2006, of 129 lawsuits mixing criminal and civil actions.^[105] AOL reinforced its efforts against phishing^[106] in early 2006 with three lawsuits^[107] seeking a total of US\$18 million under the 2005 amendments to the Virginia Computer Crimes Act,^{[108][109]} and Earthlink has joined in by helping to

identify six men subsequently charged with phishing fraud in Connecticut.^[110]

In January 2007, Jeffrey Brett Goodin of California became the first defendant convicted by a jury under the provisions of the CAN-SPAM Act of 2003. He was found guilty of sending thousands of e-mails to America Online users, while posing as AOL's billing department, which prompted customers to submit personal and credit card information. Facing a possible 101 years in prison for the CAN-SPAM violation and ten other counts including wire fraud, the unauthorized use of credit cards, and the misuse of AOL's trademark, he was sentenced to serve 70 months. Goodin had been in custody since failing to appear for an earlier court hearing and began serving his prison term immediately.^{[111][112][113][114]}

See also

- Advanced Persistent Threat
- Anti-phishing software
- Anti-Phishing Working Group
- Brandjacking
- Certificate authority
- Confidence trick
- E-mail spoofing
- FBI
- Hacker (computer security)
- In-session phishing
- Internet fraud
- Penetration test
- Pharming
- PhishTank
- SiteKey
- SMiShing
- Social engineering
- Spy-phishing
- Tabnabbing
- Vishing
- White collar crime
- Wire fraud