06
2009

Index

digicert®
Your Success is Built on Trust™

Phishing

A Primer on What Phishing is and How it Works

This white paper explains how phishing works and how it can be combated.

Approximately 85% of phishing attacks target financial institutions and payment services.

"Phishing Activity Trends Report - 2nd Half 2008"

Anti-Phishing Working Group (APWG)

Over 80% of domains used for phishing are compromised or hacked domains. (Only 3.5% of domain names used for phishing contain or use a brand name or misspelling.)

"Global Phishing Survey"

APWG

Most phishing web sites are active for about 20 hours until they are taken down.

"Temporal Correlations Between Spam and Phishing Websites"

Tyler Moore, Richard Clayton and Henry Stern

What is Phishing?

Phishing is just one of the many ways that the Internet can be used to get people to unknowingly provide their personal financial information to fraudsters. A phishing attack is most often initiated with a special type of spam (unsolicited email) containing a link to a misleading domain name, which appears to be a legitimate site. The email tricks the recipient into visiting the spoofed web site—one that mimics a site where the person would normally feel comfortable entering a username and password or other personal information.

Phishing has also been explained as leveraging or exploiting the design of web pages in a social engineering attack that tricks the user into thinking that they are in a legitimate and secure web session with a trusted site. Actually, the phishing site is designed to install malicious software or acquire personal information, including credit card numbers, personal identification numbers (PINs), social security numbers, banking numbers, and passwords. (Figure 1 is an actual example of an input form from one of these phishing sites.) This information is then used by the phisher for identity theft, to steal money, or to commit other fraudulent schemes.

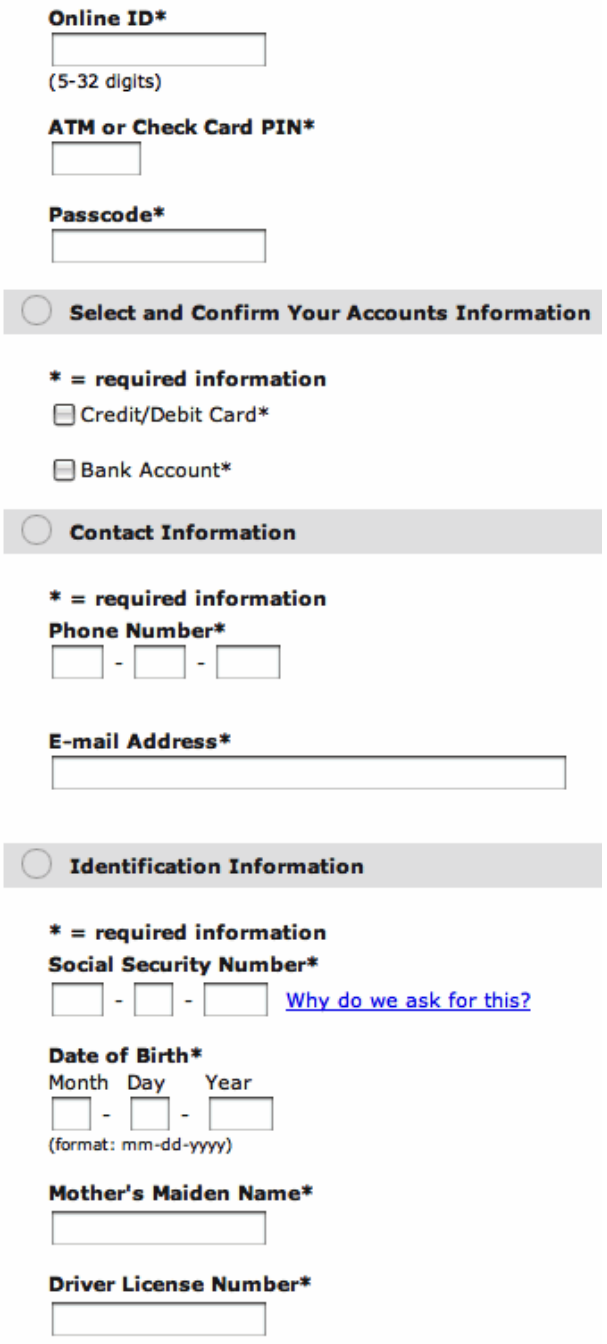

Figure 1 - Traditional Phishing Attempt

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

Phishing Continued

Examples

Here are some examples of how phishing is used. In January 2009 Bryan Rutberg was tricked into providing the password to his Facebook account. He was likely the victim of a spear phishing attack. (See sidebar.) Rutberg suspects that he responded to an email that asked him to click on a link to his Facebook account. When he clicked on the link he was actually taken to a fake web page that looked like Facebook where he entered his username and password.

The attacker then took over Rutberg's account and sent messages telling his friends that he had been robbed and asking them to send money to Western Union's branch in London. Thinking Rutberg was in need of cash, his friend sent the money. Rutberg's friend was an indirect victim of phishing and a direct victim of a scam similar to the "Nigerian" or 419 scam. These scams are directed to "reliable and trustworthy" people.

Computer users often use the same user-name and password to access a number of websites, including banking, credit card and PayPal accounts. In a variation of the example above, using the same username and password, the attacker is able to access and transfer money from the user's bank account to an intermediary's account - a money mule - who forwards the funds out of their own account to the attacker who is located in another country. The money mule gets to keep a percentage of the money as a commission. The money mule performs this money laundering task either unwittingly or as an accomplice.

In another attack, thousands of bogus subpoenas from the U.S. District Court in San Diego were "served" by email on corporate executives. The email contained an image of the official seal from the court and contained a link, supposedly to download a copy of the entire subpoena. However, when a recipient clicked on the link, key-logging software was installed on the user's computer instead. This is called a "whaling" attack. (See sidebar.)

Damage to Brand and Consumer Trust

Successful phishing attempts result in actual harm to the customer—identity theft, interception of confidential data, monetary loss, etc., but phishing also erodes trust even when systems are not compromised.

Phishing often targets and leverages the trusted brands of well-known entities like banks, payment services, social networking sites, and other places where users are likely to have an online account.

Brand owners suffer infringement to their intellectual property—trademarks and copyrights—and the good will of their businesses. Many phishing site URLs contain the name of the brand they are targeting—as examples:

- domain name - www.bank-z.com
- subdomain - bank-z.example.com
- as part of the path - /bank-z

Top targets of phishing as of the date of this white paper include: PayPal, eBay, Bank of America, HSBC Group, Google, Alliance Bank, Facebook, the Internal Revenue Service, JPMorgan Chase, Wells Fargo and Barclays - http://www.phishtank.com

According to the Online Trust Alliance (OTA), improved security is essential to enhancing online consumer trust. The OTA has announced guidelines to "prevent, detect and remediate threats and business practices that can compromise consumers' online trust and confidence, including their identity and privacy." Brand owners are encouraged to:

- Ensure implementation of protection against phishing, spam, viruses and malware including but not limited to anti-spyware, anti-malware, take-down services and fraud monitoring programs.
- Upgrade Existing Secure Socket Layer (SSL) certificates to Extended Validation SSL Certificates (EV SSL) for all ecommerce or online banking sites.

https://otalliance.org/resources/principles.html

Spear Phishing

"Spear phishing" is targeted communication toward employees or members of a certain organization or online group. Emails are customized with information publicly available on web sites like Facebook or MySpace. The emails then direct people to a fake login page.

Whaling

"Whaling" is phishing that is targeted at corporate executives, affluent people and other "big phish." Like spear phishing, whaling emails often are customized with information directed to the recipient (name and other personal information) and sent to a relatively small group of people.

Brand Owner Vigilance

Phishing site takedown is much more efficient when the actual brand owner is aware. The average uptime for phishing websites hosted on compromised machines and free web-hosting services drops from about 50 hours to about 4 hours when the brand owner is aware and becomes involved in takedown efforts.

"The Impact of Incentives on Notice and Take-down"

Tyler Moore

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

Use of Malicious Software

The Increasing Complexity of Malware

Phishing is increasingly perpetrated with the use of specially designed malicious code— "malware." This custom code comes in the form of worms, viruses, Trojan horses, spyware, key loggers and other routines that are designed to perform a variety of tasks. Some phishing malware propagates as viruses (code that spreads itself by infecting other programs) or as worms (self-spreading computer programs). These programs create an army of "zombie computers" that are centrally controlled as part of a "botnet" with the goal of "monetizing" the control over the infected systems - to turn such control into a source of revenue for the phisher.

Malware Installation

Another deceptive practice is to trick the person into thinking they need to install software—which is really malware that then captures data from the user's computer or otherwise facilitates the success of the phishing attack by infecting the target system.

For example, in late 2006 the MySpace XSS QuickTime Worm infected MySpace users' accounts with a malicious embedded QuickTime video. Links in the user's page were replaced with links to phishing sites that were designed to steal login details.

Most anti-virus programs use a method of identifying malware by checking for virus signatures or file patterns. Phishing malware is becoming more sophisticated in an effort to avoid detection by anti-virus programs and by companies that provide computer security services. These obfuscation techniques include:

- encryption of the code to increase the time needed to reverse-engineer the malware's operations, and
- self-modification and polymorphism, where the code and the decryption module change each time to avoid signature-based detection.

The Conficker Worm

In late 2008 a very sophisticated worm was released on the Internet. The Conficker worm, as it has come to be called, contains a variety of techniques and attack vectors. According to research conducted by SRI International http://mtc.sri.com/Conficker/ and others http://www.confickerworkinggroup.org, Conficker first gets its hold on unpatched Windows machines by executing unauthenticated code over port 445/TCP. It then installs itself as a randomly named dynamically linked library (DLL) in the Windows system32 directory and runs as part of svchost.exe automatically every time the computer is started. It opens up a port through the firewall as a back door and attempts to scan IP addresses and infect other machines. It also attacks local machines using NetBIOS password cracking and by infecting connected USB storage devices.

Conficker routinely attempts to download digitally signed updates of itself. It has a domain name generation engine that creates 50,000 potential domain names and then randomly selects 500 of those to contact each day, i.e., a daily rendezvous. If there are no updates it sleeps for 24 hours, otherwise it downloads and checks the digital signature of the file downloaded (so only the authors of Conficker can control the army of compromised machines). It also disables all anti-virus and patch updating services, safe-boot mode, and restore points.

So far Conficker has been used to download and install "scareware" - AntivirusXP2 2008 and Spyware Protect 2009 - and spambots (Waladec). According to Kaspersky Labs, it currently infects approximately 6 million machines. Now that Conficker has established a robust botnet, it is only a matter of time before it, or a subsequent variant of Conficker, is used as part of a phishing attack.

A Trojan horse is a program that appears harmless and is intentionally executed by the user without the user being aware of the malicious effects of the code hidden inside the program.

Many phishing emails originate from botnets - compromised computers that act as zombies to send spoofed emails to unsuspecting recipients.

Each subsequent victim is then subject to the same malware that infects his or her computer which becomes another zombie in the botnet.

In a small though increasing percentage of cases, a "rock-phish" or "fast-flux" system is set up where numerous compromised machines act as proxy web servers to hide the true location of the attacker. Compromised hosts are given a new set of IP addresses every few minutes so that someone connecting gets a different machine each time. These machines act as redirectors of requests and data to and from backend servers, which actually serve the content.

http://www.ecrimeresearch.org/ 2007/proceedings/p1_moore.pdf

APWG

http://www.honeynet.org/papers/ff

The Honeynet Project

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

Technical Exploits that Enable Phishing

Man-in-the-Middle / Man-in-the-Browser

Phishing can also consist of technical network attacks where the spoofed web site is part of a man-in-the-middle (MITM) / man-in-the-browser attack (Figure 2). More particularly, MITM attacks are accomplished by redirecting the visitor to a fraudulent server. Besides emails with clever links, this can be accomplished by redirecting the user through a false wireless access point or DNS poisoning. As illustrated in Figure 2, the fraudulent server then acts as a proxy and intercepts communications between the browser and the intended website.

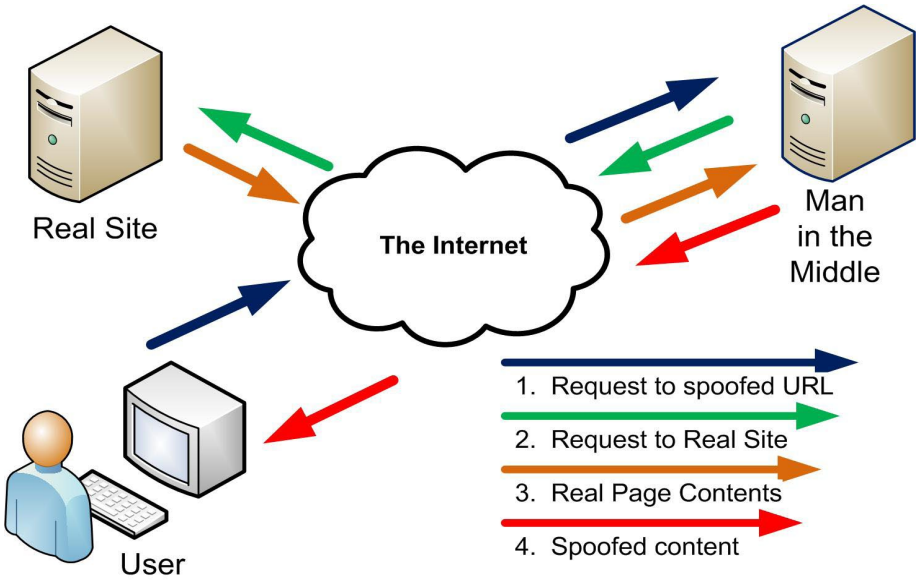

Figure 2 - A Man in the Middle Attack

Cross-site Scripting Attacks

Another means of attack is to compromise the web server and provide malicious code that is delivered via the legitimate (although compromised) server itself. This is referred to as cross-site scripting (XSS). See Figure 3. When the victim visits the page, he or she is presented with content that has been 'injected' into the page through XSS. The script runs on the client machine and sends personal data to the attacker.

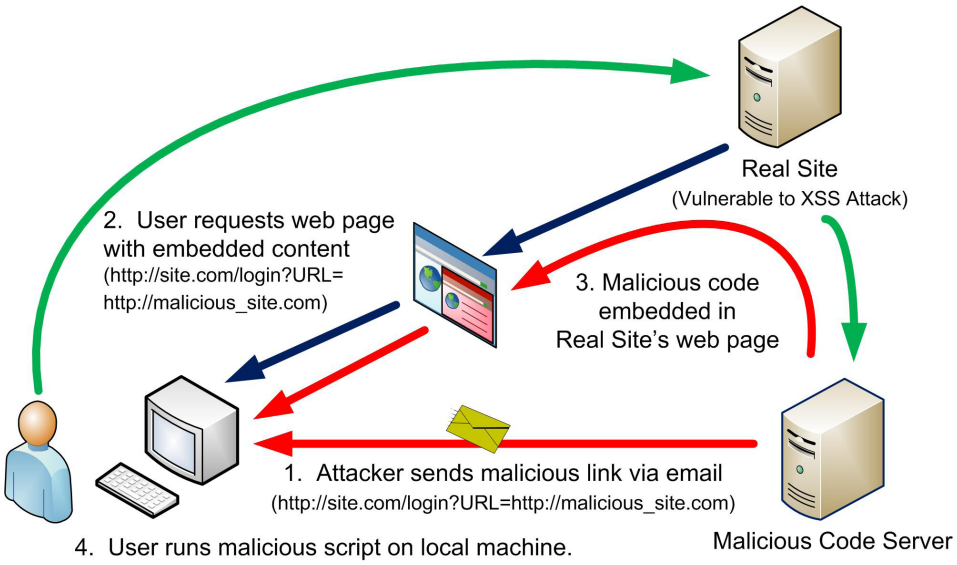

Figure 3 – A Cross-Site Scripting Attack

Pharming

The redirecting of unknowing users to another IP address for a fraudulent site where information is captured (even though the users type in the correct web site) is called "pharming." Pharming is accomplished through DNS cache poisoning (changing the hosts file on a victim's computer) or the DNS table in a vulnerable DNS server or in some cases through hijacking or using a rogue DNS server.

Nearly all phishing sites launch immediately upon registration of the domain. The few that exist for long periods of time before being used for phishing are often the victims of hacking (server compromise) or domain hijacking.

A number of tests can be run to determine whether a site is susceptible to cross-site scripting attacks. For example, XSS-Me is available at: http://labs.securitycompass.com/index.php/exploit-me/ and an XSS scanner is also available from Acunetix http://www.acunetix.com/cross-site-scripting/scanner.htm.

Internet Explorer 8 has an XSS filter to make Type I (reflected XSS) attacks more difficult to mount. However, other types are still possible. See http://www.xssed.com/xssinfo.

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

Identity Vetting Combats Phishing

How is the Domain Registration System used in phishing?

Phishers are acutely profit driven. Like spam, it is a numbers game - the fraudster knows that for the millions of emails sent, some unlucky person will respond to the bait and get caught. They seek the most profitable phishing attacks. For example, they will find a way to get a misleading domain name through the registration process with the least amount of scrutiny or they will use a domain registrar that will provide them with the longest uptime. These domain registrars need to implement better identity vetting and quicker take-down processes to make it more difficult for phishers to succeed.

Subdomain Registries

Phishing sites can also consist of subdomains of other upper-level domains. In other words, certain businesses, often referred to as "subdomain registries," provide their customers with DNS service and allow their customers to create a "name" or subdomain (e.g., http://subdomain.domain.com).

These subdomains are difficult to control because there is no WHOIS information available. Instead, DNS servers are completely reliant upon the subdomain service provider. Often these subdomain registries do not collect complete and accurate contact information of their customers. For fear of offending customers, some of these subdomain registries are difficult to work with when a phishing site needs to be taken down. Also, the fact that there are many legitimate subdomain sites beneath the upper level domain means that suspension of the upper level domain by the registrar cannot be done without harming innocent businesses.

How can Certificate Authorities combat phishing?

Certificate Authorities like DigiCert rely on the contact information maintained by domain registrars to determine domain ownership. They check on information about the owner of the domain and confirm that the applicant for a certificate is authorized to apply for and obtain the certificate.

A negligent Certificate Authority (CA) could issue a certificate to a fraudulent site. A spoofed domain name could go unnoticed, so there may even be a valid certificate issued to the MITM proxy. To address this concern, validation personnel should be trained to look for similar, misleading domain names or ones that would otherwise be considered "high risk." Also, because security is added to the server certificate when the CA conducts more extensive checks on the organization applying for the certificate, the use of domain-only validated (DV) certificates is therefore discouraged.

Use of Extended Validation (EV) digital certificates are part of a multilayered solution to combat phishing. The issuing CA performs an extensive check on the identity of the entity requesting the certificate. As illustrated in Figure 4, EV certificates activate the green bar in browser software that signals to site visitors that they are in a secure session with a validated site/organization. As illustrated in Figure 5, warnings pop up in Mozilla Firefox and Opera if a phishing site is encountered. Many other browsers have similar antiphishing features.

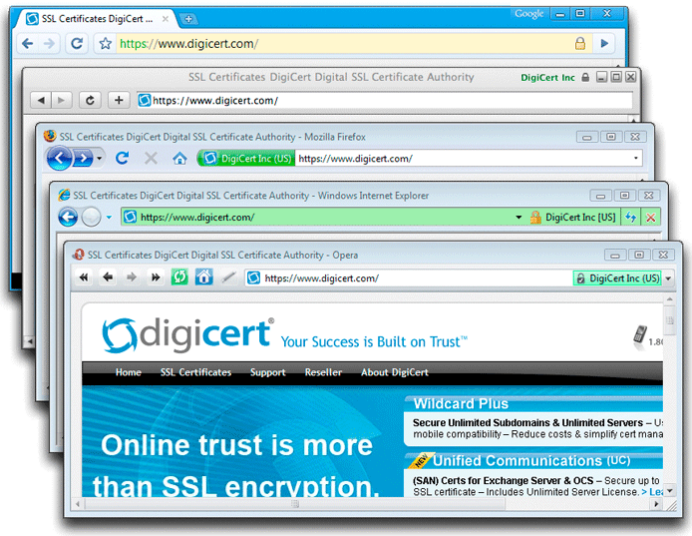

Figure 4 – Green URL in EV-Enabled Browsers

Domain Hijacking

The successful hijacking of a domain account from its legitimate owner is not considered phishing - it is considered domain hijacking. Phishing, however, can be a means by which an attacker hijacks the domain account itself. Also known as "registrar impersonation," these phishing attacks consist of an email that purports to come from the domain registrar. The phisher is then able to take control over the entire domain.

In addition to improving the identity validation and recordkeeping processes of subdomain registries, phishing could be combated through a contractual requirement that each party police the activities of its "customers" in the domain name space it controls.

While it is unlikely that a fraudster will register a domain and then go through the process of identity vetting required to obtain a digital certificate, this might occur with domain-only validated (DV) certificates that some vendors (not DigiCert) issue in a matter of minutes. Low authentication DV certificates pose a substantial threat.

Conversely, the EV process, developed by the CA Browser Forum, requires that the CA verify the legal, physical and operational existence of the organization and that the applicant is the registered holder, or has exclusive control, of the domain.

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com

Anti-Phishing Tips

What can customers do to defend themselves effectively from phishing attempts?

Phishing will be successful as long as customers are unaware of the threats. Customers should be advised:

- Upgrade your software (OS and browser). The latest versions of Microsoft's, Mozilla's and other vendors' browsers come equipped with anti-phishing filters. (See Fig. 5.)
- Learn when to trust emails sent from your trusted organizations. For example, instead of relying on email alone, check online to see if there are any important messages to you inside your trusted site.
- Instead of clicking on a link in an email, open a new browser page and type in the address / Uniform Resource Locator (URL) for the site that you are intending to visit. While connected, compare the name of the web site in the address bar with the one you trust.
- Delete suspicious messages before opening.
- Only accept trusted certificates - don't ignore browser warnings
- Be wary of (or don't click on) links that will take you to an unfamiliar site or a mere IP address.
- Look for the green address bar activated by an Extended Validation Certificate. Click on the lock icon and read what it says.
- Forward phishing emails to spam@uce.gov, to the organization being impersonated, and to: reportphishing@antiphishing.org.

What else can be done to combat phishing?

Obviously, Companies should protect themselves by securing their own machines and preventing their domains from being hijacked. They should also reduce phishing site uptime by policing brands and notifying anti-phishing service providers as soon as they discover that their brand is being phished.

Site authentication for consumers is also important. Some sites have implemented authentication mechanisms like "personal security images" and phrases that convey familiarity, uniqueness, and authenticate the site to the customer. Similarly, EV Certificates provide another recommended means of providing site authentication.

A layered approach is essential - patch and protect machines, improve the domain name registration process, implement EV Certificates, and take down phishing sites before they are successful.

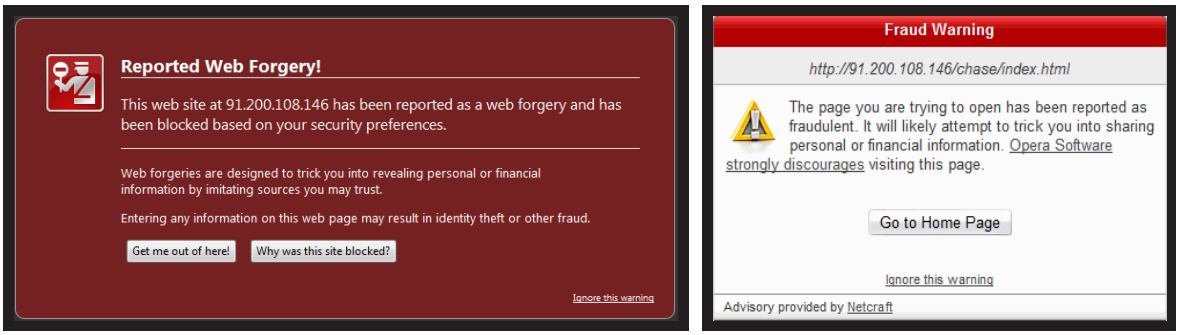

Figure 5 – Phishing Alert Warning Pages

DigiCert, Inc. <http://www.digicert.com> is a leading provider of enterprise-grade, high-assurance, 256-bit SSL Certificates trusted by many national and state governments, educational and medical institutions, and Fortune 500 companies around the world. Located in Lindon, Utah, DigiCert is a WebTrust Certified Certificate Authority and a member of the CA/Browser Forum, the W3C Consortium, the Online Trust Alliance and the Anti-Phishing Working Group (APWG). DigiCert offers Extended Validation Certificates.

EV Certificates

EV SSL Certificates provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

"Make it more difficult to mount phishing and other online identity fraud attacks using SSL certificates;

Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users; and

Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject."

CAB Forum's EV Guidelines
http://cabforum.org

Additional Resources

PhishTank
http://www.phishtank.com

Anti-Phishing Working Group
http://www.antiphishing.org

Online Trust Alliance
https://www.otalliance.org

CAB Forum
http://cabforum.org

Internet Crime Complaint Ctr.
http://www.ic3.gov

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
www.digicert.com