What to Do If Your Website Has Been Hacked by Phishers

An APWG Industry Advisory

APWG

Committed to Wiping Out Internet Scams and Fraud

January 2009

Correspondent Authors Contact Data:
Suzy Clarke, Suzy.Clarke@asb.co.nz
Dave Piscitello, dave.piscitello@icann.org

Principal Investigators:
Suzy Clarke, ASB Bank
Dave Piscitello, ICANN

Contributing Researchers

Joe St Sauver, PhD, University of Oregon
Paul Laudanski, Microsoft
David Zamler, Federation of Security Professionals
Ryan Macfarlane, FBI
Paul Nankervis, National Australia Bank
Darren Bilby, Google

Overview

Some phishers use compromised computers to host malicious or illegal activities, including identity theft, fraudulent financial activities, as well as collecting personal information and business identities from their victims for future use. Others attack or "hack" into and gain administrative control over the legitimate web sites[1] of businesses and organizations of all sizes. Such hacked web sites disguise the bad acts the phishers perform. More importantly, web site hackers are fully aware that the web sites they hack and "own" are reputably legitimate. Law enforcement and anti-phishing responders respect and operate under established business, technical, and legal constraints when they seek to remedy or take down hacked web sites. These measures protect legitimate web site operators but unfortunately serve the attacker as well by extending the duration of the attack.

The Anti-Phishing Working Group (APWG) offers this document as a reference guide for any web site owner or operator who suspects, discovers, or receives notification that its web site is being used to host a phishing site. The document explains important incident response measures to take in the areas of identification, notification, containment, recovery, restoration, and follow-up when an attack is suspected or confirmed.

This document serves a guideline for web site owners. The list of responses describe here is not exhaustive. We provide a list of complementary resources to help web site owners learn more about each recommended action. In several cases, the document mentions software that a web site owner may find useful when attempting to perform recommended actions. The software lists, too, are not exhaustive. The examples provided in these lists are representative of a very broad set of commercial and open source programming solutions. Web site owners are encouraged to research and experiment with other software as well.

Many actions will require business, technical, and legal expertise that are beyond the scope of this document. Web site owners are encouraged to discuss such matters with experts in each of these disciplines.

[1] http://www.theregister.co.uk/2007/07/10/plug_and_play_phishing/

Web Site Phishing Attack Scenarios

A web site phishing attack often begins when a phisher breaks into or "hacks" a reputably legitimate web site. By "hacking a web site," we mean that the attacker gains control of the computer (server) that hosts your web site and finds a way to either add phishing pages to the web site, change the content of the web site, or add software for execution or download to the web site.

An example of adding pages to the site is when the phisher gains control over a legitimate website like www.example.com and then adds an unauthorized page in an obscure directory such as www.example.com/~sneaky/. The phishing email—the lure that draws a victim to the phishing site—may use an image or hyperlink to disguise the fact that when the victim attempts to visit a bank, an e-merchant, or an organization's customer or Intranet portal, the victim is really visiting www.example.com/~sneaky/stealyourID.html. Attacker may take great pains to make the unauthorized page (stealyourID.html) appear identical to the impersonated web page. This deception is intentional and is designed to trick users into entering sensitive information such as user accounts, passwords, credit card numbers, or other personal information.

The following sequence illustrates a representative hacked web site response scenario.

1. A third party notifies either the web site operator or domain owner that its web site is compromised. Together, the parties attempt to verify third party's authenticity while they investigate the claim.

   Alternatively, the web site owner or operator may suspect or discover the web site phishing attack through self-examination or web site intrusion monitoring. In this case, the owner or operator initiate whatever containment actions they determine to be appropriate and proceed to step (3). (See the section entitled *Containment* for additional information.)

2. The web site owner reports the incident. The APWG strongly encourages web site owners to report the phishing URL to the APWG via email at reportphishing@antiphishing.org. (See the section entitled *Reporting* for additional information.)

3. If both the third party and the claim are legitimate, the web site owner authorizes containment and the web site operator initiates whatever

containment actions the parties have determined to be appropriate. (See the section entitled *Containment* for additional information.)

4. The web site owner and operator initiate recovery actions. Here, both parties assess the damage to identify what data and services must be recovered. The timeline assists parties in determining whether data recovery is required and whether there is any accurate data available for recovery. (See the section entitled *Recovery* for additional information.)

5. The web site owner and operator initiate restoration actions. Here, efforts focus on returning the web site to full, uncompromised, "normal" activity. (See the section entitled *Restoration* for additional information.)

6. The web site owner and operator revisit the incident to study how and why the incident occurred to determine what additional measures might be taken to reduce the possibility of future, similar incidents. (See the section entitled *Follow Up* for additional information.)

Note: (2) and (3) may occur in reverse order, depending on the organization's preparedness and how it is structured. Some organizations empower web site operators to contain without prior approval while others do not.

Many organizations outsource web site hosting to service providers. Third party web hosting providers should have their own procedures for dealing with phishing sites hosted on their servers. Ask your hosting provider to discuss these procedures with you before an event occurs. All web site owners should also make certain that the web site hosting provider is contractually obligated to notify them in the event of a hacked web site incident, and both parties should agree on a common set and order of response actions in advance. If your web site hosting provider indicates it does not have procedures in place to deal with web site phishing attacks, please refer them to this document.

Identification

Stealth, evasion, and covert operation aptly describe how phishers and other attackers compromise and remotely operate systems that host web sites.

1. How can I know if our web site has been attacked?

The most common form of identification (notice) includes **Third Party Notifications.** You may receive a notice by phone or email from an individual or organization that claims knowledge of an attack. Obtain as much information from the third party as possible, including:

a) The person's name
b) Name of their organization
c) Return contact information (phone, email, postal address, organization's web site)
d) Web page(s), including the URL (link) the party alleges to be a phish web site
e) Nature of attack (attempt to steal personal information, to complete a bogus credit card transaction, to obtain user account credentials, etc.)
f) A description of any malicious content that appears to be downloadable from your web site (e.g., spyware)

Use this information to report the incident in accordance with a predetermined incident reporting and response plan. (See the section entitled *Reporting* for additional information).

2. Can I trust third party notifications?

No, the claim may not be accurate. While a notice from third party who suggests that your website has been hacked is unsettling, remain calm. Be suspicious if the party refuses to provide the above-mentioned information to you. Do not be frightened, coerced, or otherwise socially engineered into taking any action the party recommends before you investigate the claim. Attempt to corroborate all contact information quickly and before you escalate the claim through an incident response process. Forward any court order, criminal complaint or subpoena to your own legal counsel for review.

3. How can I identify web site phishing attacks?

Organizations that proactively monitor their web sites can (and do) discover web site phishing attacks. Here are some examples of how various proactive monitoring can help you identify attacks:

a) **Traffic monitoring.** Your web site developers or your information technology (IT) staff may notice unusual access to your web site, unusual traffic volume directed at your web site, or unusual traffic emanating from your web server, or an unusual number of requests for non-existent URLs. For example, a web server devoted solely to hosting web pages that begin to transmit thousands of email messages per second merits investigation.

b) **File system inspection.** Through routine inspection, your authorized staff may identify suspicious files, directories, or executable programs; again, imagine if your staff discovers a data base of credit card information on your web server—and none of the customers are yours.

c) **Web server configuration inspection.** Through routine inspection, your authorized staff can detect unauthorized or unintended changes in web server or operating system configurations; for example, imagine if your staff discovers that your dedicated web server is hosting Internet Relay Chat (IRC) sessions.

Event logging and reporting systems are extremely important sources for identifying web site attacks. Take advantage of firewall, web server, server operating system, and server application logs. These often contain information that allows daily operations staff or incident response (IR) teams to determine how a phisher gained unauthorized access to your systems.

Attackers are fully aware of the forensic value of event logs, so it is important that you take measures to protect your log collection and reporting system from attack. Establish a secure archival and retrieval process for event logs. In addition, make copies of logs from before, during, and after an incident. These may prove invaluable at a later time, for example during subsequent investigations into the incident. Larger organizations may wish to consider a centralized (networked) logging system too. Centrally maintained logging may be less vulnerable to destruction or manipulation by attackers than "on system" logs. (See the section entitled *Follow Up* for additional discussion.)

Record the web page(s) or suspicious activity or configuration and report the incident in accordance with a predetermined incident reporting and response plan.

4. Can security assessments help identify web site phishing attacks?

Yes. Your organization or your web site hosting provider should consider routine examinations or "scans" of web servers for suspicious or known malicious programs, improperly patched components, and configurations that do not comply with applicable security (or regulatory) policies. Your staff can perform a security assessment using a web application vulnerability scanner. Free and open source examples of such tools include Backtrack, HackerGuardian, Nessus, Nikto, and Sandcat (Note: a search engine query for "web application scanners" will yield multiple trusted download sites for these and similar applications). Security consultants and auditors can perform more exhaustive assessments and can be contracted to do so on a recurring basis. Your staff can improve anti-hacking and secure web application design and programming by regularly performing scans.

A careful security assessment should compare the content on your web server against known-to-be correct versions—the content you intended to host. Eye-balling files or comparing file sizes is not sufficient: use checksums generate by applications such as Open Source Tripwire to assure that files are identical. When you perform such assessments, generate a detailed report that can be used in accordance with a predetermined incident reporting and response plan.

Once you suspect, have discovered, or been notified that your website is hosting a phishing site, report the incident, in accordance with a predetermined incident reporting and response plan.

Reporting (Notification)

1. Should I report the incident?

The exact reporting procedure and the parties to whom a phishing web site incident are disclosed may be influenced by business, regulatory, and legal responsibilities. As part of an overall security strategy, organizations that operate public-facing web sites (in particular, those that collect personal, financial, and other sensitive information) should consult with executives, communications personnel (e.g., public relations departments), and legal counsel to ask that they provide input to the incident reporting procedures that specifically address web site attacks.

2. To whom should I report it?

As you prepare your reporting procedures, consider when and how to report your incident to:

a) Anti-phishing networks
b) Anti-virus and anti-malware organizations
(In cases where you discover malicious executables or scripts)
c) CERT organizations
d) Common Vulnerability and exploit (CVE) disclosure list administrators (in cases where you discover a vulnerability or "bug" in commercial software)
e) Customers
f) Law enforcement, e.g., through the Internet Crime Complaint Center[1]
g) Regulatory compliance agencies
h) Software developers
(In cases where you discover bugs in custom application software or webware developed exclusively for your organization)
i) Any individual or organization directly affected by the phishing attack, even if they do not fit into one of the other categories listed above.
j) The general public

Some of these notifications will not always be applicable or appropriate for a particular incident. If your web site belongs to a corporation, a not-for-profit organization, a government agency, or any organization that must satisfy regulatory compliance criteria, you should report a web site phishing attack that results in a material breach to executive management or in-house legal counsel. Evidence of a web server breach that has data breach implications in the context of health care, privacy, or financial reporting regulations may instigate a full review of the compromised system to determine the extent of compromise and also to determine what, if any, compliance violations may have contributed to or resulted from the incident.

Management and legal counsel are best suited to prepare and coordinate external reporting and notification to response teams, CERTS, regulatory agencies, and law enforcement. Communications departments should be consulted prior to contacting

[1] The Internet Crime Complaint Center (IC3, http://www.ic3.gov) provides a central referring mechanism for cyber criminal complaints. IC3 accepts complaints from Internet users and refers them to appropriate (local, state, federal and international) law enforcement and regulatory agencies.

customers, the press, and general public. They have the training, skills, and relationships needed to effectively communicate information pertaining to an incident, and experience managing reactions to what may be alarming news.

Having well-documented incident reporting procedures in place typically assures that everyone in the organization understands her role in the reporting process. It minimizes confusion, delays, and errors in responding to an incident; limits worry over embarrassment and tarnish to brand; and it expedites containment, recovery, and restoration.

Incident reporting procedures may require that you contact your IT support, web hosting provider, and ISP so that all parties who participate in providing or supporting your public web presence are engaged in the response. Each party may have specific actions they need and expect you to take in addition to those outlined in this guide. Be prepared to provide all relevant information, such as logs from your web server, firewall, and operating system, as well as copies of the unauthorized content, dates, and times that you were made aware of the issue (also known as an "incident time line"). Keep a record of what information you provided, and to whom.

These administrative actions help inform the appropriate people about the incident so that you can ensure a more unified response.

APWG encourages you to report the phishing site URL to the APWG via the email address reportphishing@antiphishing.org. Reporting to this address will cause most anti-phishing organizations to receive a notification of the phishing web site. Security products, e.g., anti-phishing toolbars, will be updated with the offending URL, thus offering protection to thousands, if not millions of potential victims.

If you're unsure about whom you should report the incident to, seek advice from in-house or external legal counsel or professional incident response organizations.

Containment

Consider the following issues if you have the necessary level of (administrative) access to your web site. If you outsource web hosting, discuss containment measures in advance with your web site hosting provider to assure that you and your provider have the same response strategy or you may waste time responding "on the fly" that might otherwise be spent minimizing damage and loss.

1. Should I make a copy of the unauthorized content?

Generally, yes. Save a copy of the phishing site pages and any unauthorized content, scripts, or executable programs you discover during your analysis. These will help web site operators, system administrators, and/or an IR team to verify that the content change was unauthorized, intentional, and malicious. They may also help to determine which vulnerability let the phishers alter your website. You may wish to copy the unauthorized content as soon as you isolate and discover each page, executable program, etc.

If you or your hosting provider cannot obtain a disk copy of the system involved in the phishing, consider creating a *logical copy*, i.e., copy the files and preserve the folder structure. When creating a logical copy of files from the compromised computers, use tools such as Robocopy or the Unix cp command.

Please note that certain content—in particular content such as child pornography—poses serious legal implications if placed in the possession of persons who are not law enforcement agents or are not acting on behalf (and with full knowledge) of law enforcement. If you find any indication that illegal content is present on your system, do not make copies! Stop all investigative activities, contact the appropriate law enforcement in your jurisdiction, and follow their instructions regarding how to proceed.

2. Should I take my site offline (temporarily)?

You must decide in advance whether it's appropriate to suspend service to your website for a short period of time while you attempt to investigate the attack. Make this decision as part of defining your overall incident response handling strategy. This strategy prevents additional visitors from falling victim to the phishing scam and also prevents the phisher/attacker from remotely controlling your web site. Consult with IT and IR teams to determine ways to shut down your site without the risk of losing traces of the phisher's activities, and consult with law enforcement and applicable regulatory compliance experts to understand the implications of temporary site suspension.

You may be advised or choose to leave the site online long enough to provide incident response teams and law enforcement with an opportunity to monitor the phisher's activities. If you choose to stay online, ask your IR team or law enforcement whether you should change administrator and user passwords immediately. Some investigators may want to continue to monitor an attacker's

use of a compromised account. Discuss with your IR team whether the phisher appears sophisticated enough to have installed a program that will attempt to delete all evidence of his activities upon detection of loss of access.

3. Should I disable the unauthorized content?

If you do choose to keep your web site running, remove or disable access to the unauthorized web pages of the phishing site. Make copies of, remove and submit any malicious content to an antivirus or antispyware vendor. Redirect any visitors attempting to visit a phished page to a web page you have prepared that explains they have been tricked by a phishing email and that you have removed the page they were lured into visiting. The APWG provides a standard "you've been phished!" redirection page and instructions for its use at http://education.apwg.org/r/about.html. This strategy will prevent further use of the phishing site, keep your customers informed, keep your web site online for real time analysis, and afford you additional time to perform containment actions.

4. Are there right and wrong ways to make copies of content?

How you make copies matters. File system-based copies (e.g., copying files from the compromised system to removable media or to a network file share) do not have the forensic and evidentiary value as a full (sector by sector) disk or partition copy. The Unix `dd` and WinDD utilities, NFGDump, and SelfImage are examples of utilities you can use to create "clone" images of the entire hard disk and partition where you discovered the phisher's unauthorized content. It is often useful (or necessary) to copy content from the compromised system using a bootable rescue CD (also called Live CD). Programs such as the Trinity Rescue Kit, Knoppix, Helix from www.e-fense.com or SLAX are examples of such utilities. These and other useful forensic software tools are freely available under the GNU GPL or similar "open source" licenses (a search engine query will yield multiple download sites for these applications, please exercise care and verify both the tool and its origin).

Save copies of your web site and all event logs that may be useful for incident analysis offline, e.g., on a DVD, CD, or on increasingly affordable portable hard drive devices. Include (digitally signed) checksums or hashes of your web pages on this DVD/CD so that it is easy to distinguish your intended and authentic content from unauthorized substitutions and additional content. Many hash generator programs and file-system anti-tampering software are available for this purpose. Consider creating images of compromised web server operating system and application partitions for forensic analysis and follow up.

Recovery

Recovery can be a slow and costly process if you have not prepared properly in advance. Don't wait for an incident to archive your authentic content. Routinely save and archive copies of your website and logs to a location outside of the web root. Save all configuration files and maintain a careful record of configuration updates. If possible, burn all this data along with a copy of your website to a DVD, CD, or copy to a portable hard drive device or backup system.

Consider routinely creating an exact copy of your web site for backup purposes. In addition to archiving your content, create images of web server operating systems and application partitions as well. These can be especially helpful in restoring systems to a previous, known security profile; for restoring security configuration files; and for restoring operating systems to a known patch level and known set of tested and approved patches and hot fixes.

Periodically or routinely restore files from archived media to make certain that your backup procedures, media, and devices are in working order and that the backups you make do indeed restore your web site to the state you intended when designing the procedure. The restore operations described below are best performed offline, using local administration on a secured network (e.g., from behind a firewall).

1. Should I restore from backup or rebuild from scratch?

The only way to ensure that your servers are "clean" is to rebuild from original install media or to do an OS restore from known-good backups in offline mode, as recommended above. (If you cannot rebuild or restore offline, do so online but behind a firewall). Prior to restoring from a backup or rebuilding, you must determine *when* and *how* the web site was compromised. Knowing when the compromise occurred is critical because this identifies the last known-good backup of your content and other recovery images. *When* also establishes a point in time after which all archives of your web site must be treated as suspect. These may be relevant to any forensic investigation you conduct for this incident.

Determining *how* your systems were compromised before you rebuild or restore is critically important. The phisher discovered a vulnerability—a configuration error or software bug—and exploited this to obtain administrative access to the system(s) that host your web site. If you do not correct this vulnerability, the

phisher or another attacker will invariably exploit it again.

2. When should I update my software and check my configuration?

When you restore, you return your web site to a known-good state, but you are also going back in time. It is possible that patches, security updates, and configuration changes were introduced during the interim between the current date and the date of your restore images. If you are rebuilding from original media—e.g., Windows 2003 Server, OpenBSD, or Linux installation CDs—it is even more likely that your installation media are missing critical updates that were released after you obtained the media. Before you return your web site to a production environment, update all of your software to the latest versions and install all relevant patches and hot fixes. This includes patching operating systems, third-party, and custom applications that you may have installed on your systems.

It is extremely important that you verify that your web server OS and applications are configured properly. During the restore process, you may install a default configuration (common when you rebuild from scratch) or a configuration that you had modified subsequent to the date of your restore images. Perform a security assessment to verify that the restored system is configured correctly (and securely) before you return the web site to a production environment.

3. Should I change all my passwords?

When you are confident that you have restored your web site to an authentic and normal operating state, that you have installed all necessary software patches and hot fixes, and *after* you have taken measures to mitigate the vulnerabilities the phisher exploited, change all the passwords used to access accounts on the hitherto compromised system(s). The phishers may know the current passwords. It is important to acknowledge that even competent users and administrators use the same password on multiple systems (some business, some personal, and some public!), so consider whether it is appropriate to perform an extensive password reset procedure. Some organizations may also want to consider the merit of implementing multi-factor authentication, e.g., a hardware cryptographic token, to make login processes more secure.

Changing passwords on a regular basis (e.g., every 30 days) is considered a good operational practice in general and an essential practice for web and system administrators. Incidents raise awareness of lax practices and create incentives to improve both security baselines and routine maintenance schedules, so take this

opportunity to define a rigorous password security policy that not only enforces regular password changes, but minimum length (e.g., 8 characters) and complexity criteria (e.g., password must contain upper and lower case letters, numbers, and special characters). While you are focused on password management, make sure that all forms of remote authentication and logins are performed over encrypted connections.

Unless otherwise directed by a forensics team or law enforcement, change passwords immediately and then again once you believe you have completed remediation and have restored your site. This significantly reduces the risk an attacker will continue to use your account while you are attempting to remediate.

Follow-up

Organizations benefit from a post-mortem analysis of an incident. During this analysis, study the entire chronology of events leading to, during, and following the web site phishing attack.

1. What lessons have I learned?

During the follow-up process, ask, ""What would I do differently next time?" and "What processes would I change now to avoid a similar situation in future?" as well as any similarly tough questions you need to answer.

Gather web site owners, operators, service providers, IT and IR teams to share information about the incident. Take time to familiarize all parties with the anatomy of the attack. Identify characteristics of the attack that might be useful in early detection of future, similar attacks. Identify software, configuration, and operational changes that are considered appropriate and necessary to prevent similar attacks in the future.

2. How can I do better?

Web sites are prime targets for phishers. Consider the following list of recommended practices for minimizing a web site's vulnerability to attack by phishers.

a) **Server OS hardening.** "Hardening" is a process of securing an operating system so that it is difficult to attack. Use commercial and open source vulnerability scanners and security baseline analysis tools to identify

unnecessary services, accounts, and improper (exploitable) configuration settings. The Center for Internet Security offers analysis tools and security templates for commercial and open source operating systems commonly used for web server hosting.

b) **Web application hardening.** Web application hardening is a process of securing web server application software (Microsoft IIS, Apache, etc.), web applications and scripts, and dynamic content against attacks. Again, use commercial and open source web vulnerability scanners to identify improper configuration settings and exploitable content. Consider using a commercial or open source web application firewall such as ModSecurity provide in-line, real time examination of incoming web traffic for attack patterns and anomalies.

c) **Patch management.** Maintain current patch levels on all operating systems and applications used for your web site.

d) **Secure programming, safe scripting.** Do not use executable programs without verifying the authenticity and trustworthiness of the developer and the integrity of the code itself. The Open Web Application Security Project (OWASP) is a useful source for learning about secure programming and safe scripting (for more information on OWASP, see the *References* section on page 17). Only use executable programs from trusted commercial vendors and trusted open source developers whose work products are typically MD5 hashed and digitally signed. Do not use even the most trivial scripts without reviewing the source: be certain you know exactly what the script does, and everything it does, before you employ it.

e) **Compartmentalize.** Running multiple application servers—DNS, mail, web, Active Directory—on a common server is a recipe for an incident. Operating database servers containing sensitive information and public servers on a common LAN segment is a companion recipe for an incident. Create security domains within your network and separate these with security systems (e.g., firewalls) so that successful attacks against one server or service can be contained.

f) **Routine Self-examination.** Perform regular network, host, and web vulnerability and penetration tests. If possible, have an independent, experienced, and certified party perform a security or vulnerability assessment on systems that support your web site.

g) **Implement best practices for ingress and egress firewall filtering.** Restrict traffic flow at firewalls as tightly as practical. Only allow access to TCP or UDP ports where your authorized services are listening, and further restrict flows to the IP addresses of the systems on which you are hosting listening services. Restrict outbound traffic flows from servers as well. Where possible, only allow servers to establish outbound connections to authorized services

on designated external hosts.

h) **Logging, event reporting, log analysis, intrusion detection.** Log traffic, OS, and web application events at the "right" level of detail, taking into consideration performance, cost and the utility of information collected. Collect log and event records at a secure log server. Regularly (and securely) archive log files and routinely analyze traffic and event logs for unusual or anomalous access and activities.

i) **Proactive security measures.** Complement aggressive logging and analysis with real-time network, host, and web intrusion detection systems.

j) **Stay informed.** Operating system and web application vulnerabilities are discovered and exploited on an almost daily basis. Subscribe to a vulnerability notification service offered by regional CERTs, SANS, SecurityFocus, and other security services organizations. (For more information, see the *References* section).

Conclusions

Any security incident is disturbing. Web site phishing attacks can be frustrating, costly, and embarrassing experiences. The threat of these attacks can be greatly reduced by implementing appropriate security measures alone or with the assistance and cooperation of web hosting and Internet service providers. Equally important, the cost and embarrassment of an actual security incident can be greatly reduced by carefully planning for and implementing appropriate incident response procedures such as those described in this document.

References:

- Anti-Phishing Working Group (APWG), http://www.apwg.org
- Backtrack, http://www.remote-exploit.org/backtrack.html
- CERT Cyber Security Alerts, http://www.us-cert.gov/cas/signup.html
- Center for Internet Security, http:///www.cis.org
- Internet Crime Complaint Centre, http://www.ic3.gov
- Microsoft Baseline Security Analyzer, http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- Modsecurity, http://www.modsecurity.org/
- MyNetwatchman SecCheck tool, http://mynetwatchman.com/tools/sc/
- Open Soure Tripwire, http://www.tripwire.org
- Phish Tank, http://www.phishtank.com/
- Phishing Reporting Networks, http://www.phishreport.net
- Robocopy, http://technet.microsoft.com/en-us/library/cc733145.aspx
- SANS Consensus Security Alert, http://www.sans.org/newsletters/risk/

- Secunia Personal Software Inspector (PSI), http://www.secunia.com/vulnerability_scanning/personal/
- SecurityFocus Newsletter, http://www.securityfocus.com/newsletters
- SourceForge (Open Source Repository), http://www.sourceforge.net
- Open Web Application Security Project (OWASP), http://www.owasp.org/index.php/Main_Page