

Insight to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter



Warning on Phishing attacks in the State:

From Infragard: An avalanche of phishing is now roaring through Microsoft's MSN network, luring recipients to a page that asks for their MSN login data. Those who respond will find themselves on a page displaying a few photographs, which are linked to search queries. Shortly thereafter, all the account holder's friends are sent messages containing URLs that take them to similar pages. The small print of the "Terms of Use" or "Privacy Policy" gives the game away. It's stated there, quite openly, that the access data will be used in order to show friends "new, entertaining pages". It claims not to be a phishing site because, the use made of the data is precisely as described.

Data Breach (written by MS-ISAC)

What is a Data Breach?

Data breach generally refers to instances where information has been subject to unauthorized access, often where the information is lost, stolen or hacked into. This is of particular concern when that information is private, sensitive, or confidential. Organizations and individuals have the responsibility of protecting the information in their care and proper safekeeping of this data is vital. Failure to do so can result not only in a breach, but also result in damage to reputation, significant fines or loss of revenue, and other negative consequences.

Data breaches are occurring all too frequently, and they can occur in large or small organizations, in the public and private sectors. The scope of this issue can be evidenced by the fact that more than 227 million records nationwide have been involved in a breach since February 2005. This figure represents only those that have been reported, so it may reflect only a portion of the actual occurrences. This is an issue that everyone must be aware of and take steps to mitigate.

In addition to data breach concerns, we

must also recognize that data manipulation is a potential threat. If we cannot trust the integrity of our data, and know that it has not been altered inappropriately, our ability to carry out our mission and serve our customers becomes impaired.



Some examples of data that must be protected include the following:

- Customer or employee information with names, addresses, Social Security numbers, credit card numbers, passwords and other identity-related information
- Intellectual property
- Financial information
- Health records of individuals

How is Data Compromised or Disclosed?

Attempts by hackers to steal names, Social Security numbers, credit card accounts and other information is one method of obtaining data. (cont pg 2)

Web Browser Attacks (Written by MS-ISAC)

First: What is a Web Browser?

The web browser is a software application that allows the user to view and interact with content on a webpage, such as text, graphics or other material.¹ It is a very popular method by which users access



the Internet. There are a number of different web browsers-- Internet Explorer, Firefox, Opera, and Safari are the most prevalent. Plug-ins, also known as add-ons, are applications that extend the functionality of browsers. Some of the more familiar plug-ins include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, RealOne Player and Acrobat Reader. Based (cont pg 3)

In this Issue:

Data Breach	1,2
Web Browser Attacks	1,3, 4
Security Hints	all
Security Links	4

InsighT to Security

Data Breach (continued fm pg 1)

“ Of those incidents, 18 percent stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods....”

Warning:
Do NOT believe in e-mailed warnings about viruses or other security risks that ask you to forward them on to all your friends or co-workers. Check with your IT personnel or go to www.snopes.com

Security shouldn't slow you down, it should make you more confident as you move forward.



Attackers may use social engineering, phishing or other similar attempts to gain access. These activities can translate into very large sums of revenue for those in the organized crime world. While very sophisticated techniques are sometimes used to steal sensitive data, one of the most common threats comes from within the organization itself. According to Deloitte's 2007 Global Security Survey, 65 percent of respondents reported repeated external breaches. Of those incidents, 18 percent stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods.

The loss or theft of data is not limited to electronic data loss or computer hacking. Other possibilities include physical loss of hard copy documents, theft or loss of laptops, tapes and flash-drive devices or improper disposal of hard copy documents.

Are there Laws or Regulations to Protect Data?

There are numerous laws and regulations to regulate how organizations must handle and protect sensitive information. Some of the most notable include the following:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Security Standard
- Gramm-Leach-Bliley Act (GLBA applies only to financial institutions)
- Sarbanes-Oxley Act (SOX applies only to public companies)

There are Breach Notification Laws currently in place in forty-two states and the District of Columbia which govern the notification of an individual whose personal information has, or may have been disclosed.

What Can I Do?

Organizations and individuals must take proactive measures to minimize the risk of data breach. Everyone in an organization has a role in protecting information. The following are examples of steps you can take to help prevent data disclosure:

- Follow your organization's cyber/information security policies;
- Know how your organization has classified information and adhere to the appropriate controls in place;
- Follow proper procedures for the destruction or disposal of media that contain sensitive data;
- Participate in security awareness training.

Remember, cyber security is everyone's responsibility. Don't be the weak link in the chain.

To learn more about protecting information visit the following online resources:

MS ISAC Monthly Cyber Security Tips: www.msisac.org/awareness/news

US CERT: www.us-cert.gov/reading_room

OnGuard Online: www.onguardonline.gov/topics.html

Privacy Rights Clearinghouse: www.privacyrights.org

Web Browser Attacks (continued from Page 1)

How Can Your Browser Put You At Risk?

According to a recent study, approximately 45% of people surfing the Internet were not utilizing the most secure version of their web browser.² Like other software, without the appropriate security patches applied, web browsers are vulnerable to attack or exploit. A fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins are not fully patched. It's important to remember that plug-ins are not automatically patched when the browser is patched.



Traditionally, browser-based attacks originated from "bad" web-sites but due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors.



Hackers add scripts that do not change the website's appearance. These scripts may "silently" redirect you to another web site without you even knowing about it. This redirect to another web site may cause malicious programs to be downloaded to your computer. These programs are generally designed to allow remote control of your computer by the attacker and to capture personal information, often related to obtaining credit card, banking information and data used for identify theft.

In April 2008 Panda Labs, a computer security and anti-virus publisher, announced that more than 280,000 web sites had been altered to redirect computers to malicious websites which would attack them in a variety of different ways. The SANS Institute, a computer security research and training organization, recently declared browser attacks to be "Top Cyber Security Menace" for 2008.

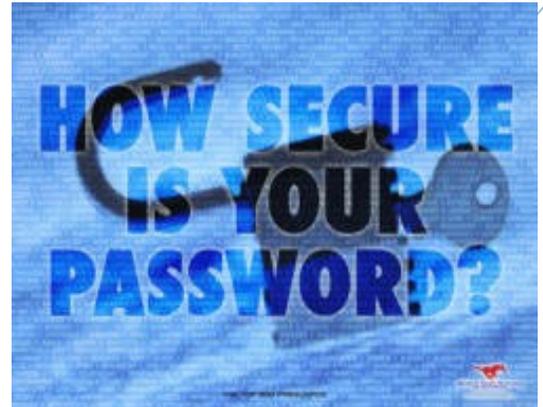
It's not just desktop or laptop computers that are vulnerable. As their popularity increases, smart phones such as Blackberries and iPhones may become targets of browser based attacks because of the built in browsers technology and Internet access.



Clearly users must be aware of the issues and take proactive measures.

What Can You Do To Protect Yourself From Browser Attacks?

There are a number of steps that we can take, most of which your IT Department may have implemented at work, but which also apply equally to your home computer. (cont on page 4)



Hacker Safe promises, often lead you into a false sense of security, making you an even better target for the hackers. Hackers love to break into "Hacker Safe" sites.

650 W State St
Boise ID 83720

Phone: 208-332-1851

E-mail: terry.pobst-martin@cio.idaho.gov



CHECK OUT
THESE
LINKS

Links to top Security Websites:

Good websites to surf:

<http://www.sans.org/>

<http://www.cert.org/>

<http://www.msisac.org/>

<http://csrc.nist.gov/>

<http://www.issa.org/>

<http://www.infragard.net/>

<http://www.ic3.gov/>

<http://www.securityfocus.com/>

<http://www.snopes.com/>

<http://www.nationalterroralert.com/>

**Internet Security is
not an obstacle, it's
the path to freedom
and flexibility.**

Web Browser Attacks (continued from Page 3)

- Keep your browser(s) updated and patched.
- Keep your operating system updated and patched.
- Use anti-virus and antispyware software and keep them up to date.
- Keep your applications (programs) updated and patched, particularly if they work with your browser such as multi-media programs used for viewing videos.
- Install a firewall between your computer and the Internet and keep it updated and patched.
- Block pop-up windows, some of which may be malicious and hide attacks. This may block malicious software from being downloaded to your computer.
- Tighten the security settings on your browsers. Check the settings in the security, privacy, and content sections in your browser. The minimum level should be medium.

Consider disabling JavaScript, Java, and ActiveX controls.

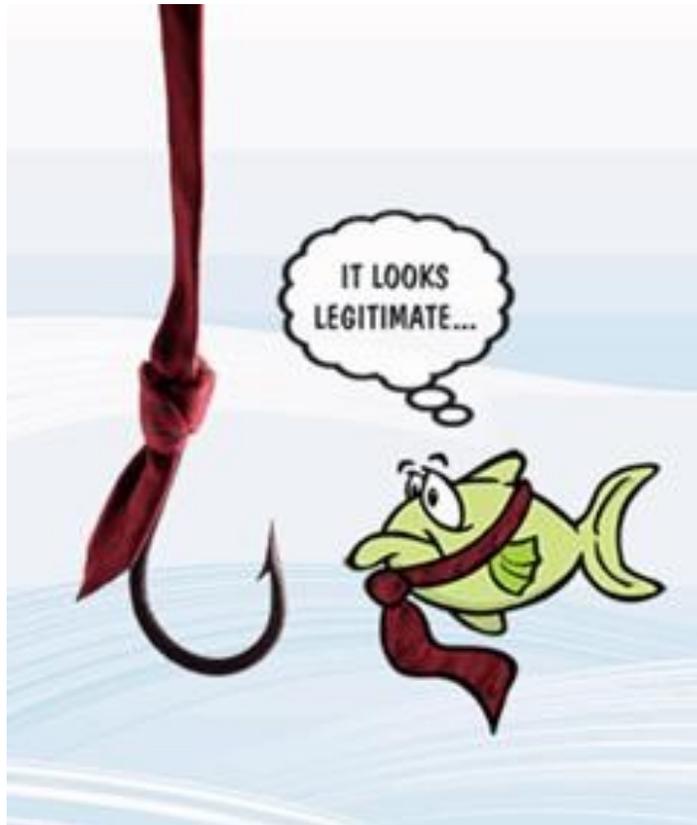
Please note, a number of these tips may impede your use of the Internet or limit what content you can access. If you find that you really need ActiveX controls or you require JavaScript be enabled, set your browser to prompt you before running scripts. If you find that you need to lower your security settings to be able to access what you need, lower them temporarily, then reset them.

1. Wikipedia, http://en.wikipedia.org/wiki/Web_browser
2. Frei, S., Dübendorfer T., Ollmann G, May M., "Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the 'insecurity iceberg' "

To learn more about browser attacks go to:

- US-CERT: <http://www.us-cert.gov/cas/tips/ST05-001.html>
- SANS Cyber Security Institute's Top Threats for 2008: <http://www.sans.org/2008menaces/>
- PC World: Hackers Increasingly Target Browsers: http://www.pcworld.com/businesscenter/article/144490/hackers_increasingly_target_browsers.html
- Computer Weekly: Attacks By Criminals on Web Browsers <http://www.computerweekly.com/Articles/2008/02/14/229406/storm-worm-is-basis-for-most-cyber-attacks-says-ibm.htm>

For more cyber security monthly tips go to:
www.msisac.org/awareness/news/



Don't fall for Phishing attacks.

Think about what you're doing.

Don't click on links in e-mails unless you're SURE they are legitimate.

Remember, banks don't send you e-mails with links or impose deadlines on your response.

Don't open e-mails that look suspiciously different.

Don't trust unusual messages—even when it appears it is from a friend.

That hook will hurt!

Contact us at 322-1505 or servicedesk@cio.idaho.gov