

Insight to Security

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

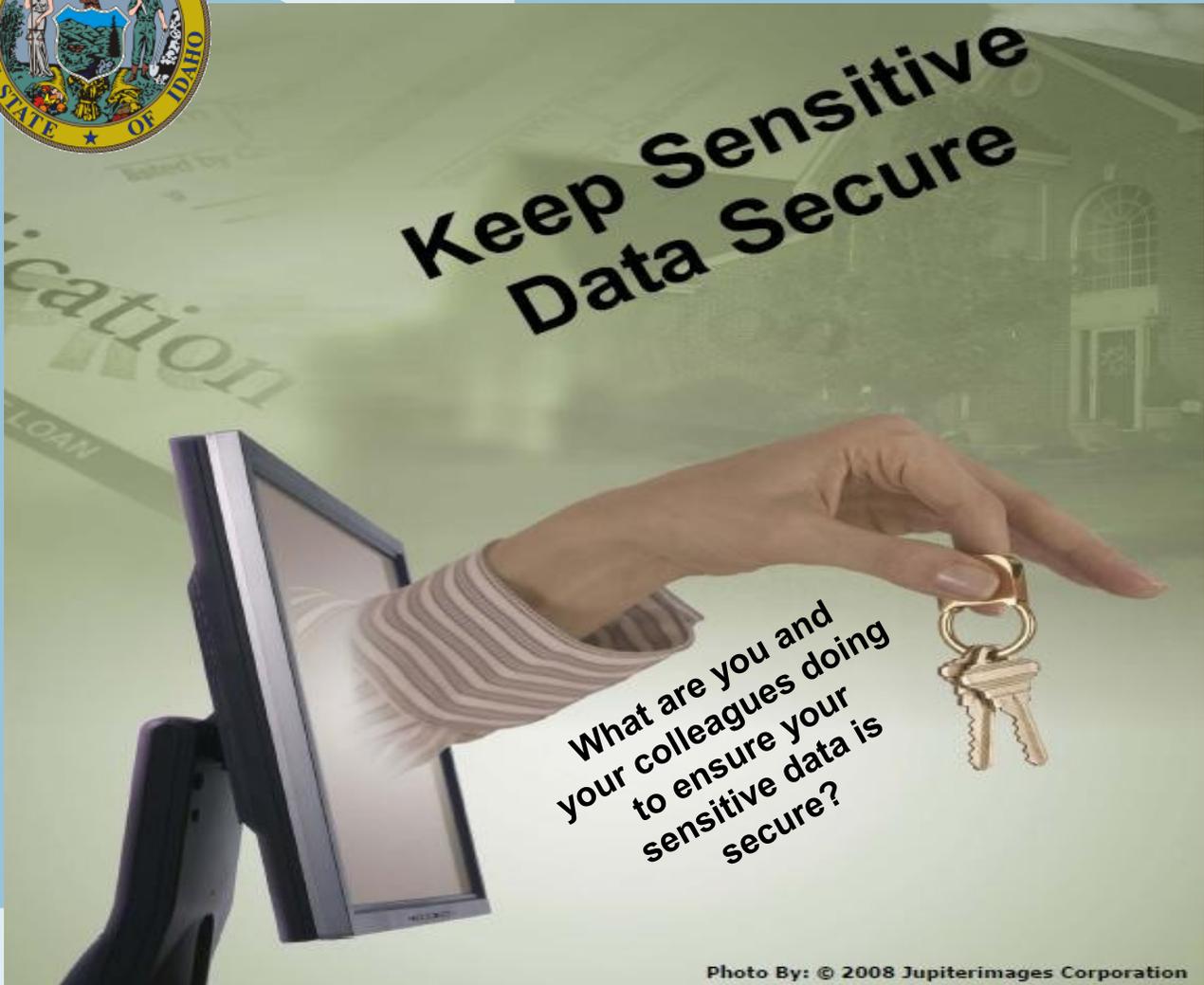


Photo By: © 2008 Jupiterimages Corporation

In this Issue:

Protecting Personal Privacy	1,2
Social Networks Info.	3
Why Info Security?	4,6
Internet Security Pledge for Kids	5
Security Bookmarks	7

Personal Privacy – How to Protect Your Information (from MS-ISAC)

As we continue to conduct more business online, such as banking, shopping and other activities, our personal information (such as name, credit card account, address, etc) is increasingly utilized. Personal information has become a frequent target for data thieves and the volume of breaches involving personal information continues to grow. According to the Privacy Rights Clearinghouse, there have been more than 240 million records containing sensitive personal information involved in security breaches to-date na-

tionally.

What Personal Information is Collected?

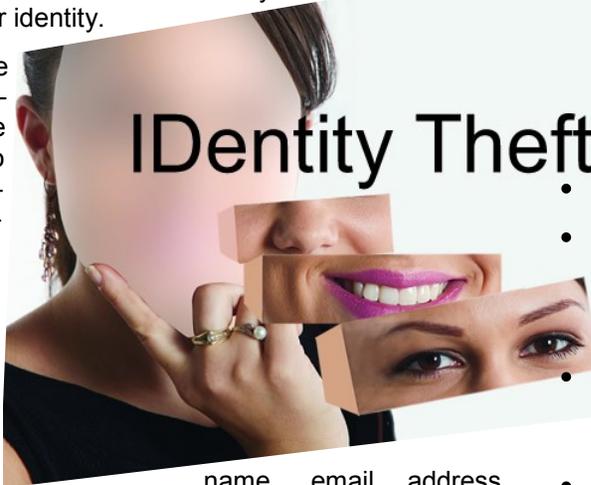
Many types of organizations are interested in obtaining and using your personal information, and it's important to know what information is being collected, by whom and how it will be used.

Websites track web users as they navigate cyberspace. Data may be collected routine (continued on page 2)

Personal Privacy – How to Protect Your Information (from page 1)

activities including:

- When you make purchases and pay bills with credit cards, you leave a data trail consisting of purchase amount, purchase type, date, and time.
- When you pay by check, data such as phone number, home address, driver's license number, etc. may often be requested about you as a result of many of your to verify your identity.
- When you use supermarket discount cards, the store is able to create a comprehensive database of everything you have purchased.
- When you surf the web, you leave a significant data trail such as your name, email address, Internet address of your computer, the name of your computer, the last time you visited that particular site, the type of browser and operating system you are using.
- When you sign up for a subscription or service (for a magazine, book or music club, professional association, warranty card, etc.) or give money to charities your personal information is often collected and stored.



information is secure during transmission.

- Periodically check your Internet browser settings (e.g. Security and Privacy) to ensure that the settings are adequate for your level and type of Internet activity.
- If you are not already using anti-spyware or adware protection software, start now. This software is designed to protect against spyware or malware designed to extract private information from your computer without your knowledge. Make sure you keep the anti-spyware or adware protection programs updated.
- Be sure to have a firewall installed and enabled.
- If you store private data on your laptop or other portable electronic devices (e.g. USB), use encryption software to protect your private data in the event the device is lost or stolen.
- Use strong passwords on all your accounts, such as a minimum of eight characters and a mix of special symbols, letters and numbers.
- To protect against identity theft, always question someone who is asking you to reveal any personally identifiable information. Find out how it will be used and whether it will be shared with others.
- Keep items with personal information in a safe place. When you discard receipts, copies of credit applications, insurance forms, health records, bank statements, or other personal documents, tear or shred them.

Protecting Your Personal Information

The following tips should be used to help you manage your personal information wisely, to help minimize its misuse, and to lessen the risk of your personal information being compromised:

Most legitimate websites include a privacy statement. This is usually a link at the bottom of the home page and details the type of personally identifiable information the site collects about its visitors, how the information is used—including with whom it may be shared—and how users can control the information that is gathered. Be sure to read the privacy statement on websites you are visiting **prior** to providing any personal information, to understand that entity's policy regarding protection of data.

- When shopping online, guard the security of your transactions by ensuring the transaction is submitted securely. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your

Order a copy of your free annual credit report. Make sure it's accurate and includes only those activities you've authorized.

References

To learn more about protecting your privacy, you may wish to visit the following sites:

Identity Theft: www.ftc.gov/bcp/menus/consumer/data/idt.shtm

Consumer Action: www.consumer-action.org

Electronic Privacy Information Center:

www.epic.org

Free Annual Credit Report: www.annualcreditreport.com



Social Networks - What You Need to Know (from MS-ISAC)

Page 3

Social networks are online communities focused on interaction among friends, families, and others who may share similar interests. Social networks allow people to communicate in many ways including email, instant messaging, forums, and blogs.

Are social networking sites

safe? Although social networking sites are not inherently dangerous, because of their open nature, and anonymity, users may not realize the potential dangers. However, every user should understand these risks and know how to address them. Some statistics indicate the following:

74% of social network users have given out at least some personal information. This information can be used to steal their identity.

83% of social networkers have downloaded content from another user. Content from untrustworthy sources can contain viruses, worms, or Trojan horses.

The following are some examples of the potential threats that exist on social networking sites:

Identity Thieves try to find out all they can about you so they can steal your identity, use your credit cards, or create new credit cards and loans in your name. There are millions of identity theft victims each year.

Predators prowl the Internet looking for victims. They rely on the anonymous nature of the Internet to hide their true identity and malicious intent.

Con-artists will try to trick you into giving them money. They may claim to be with

charities or have a great investment opportunity for you. Remember – if it sounds too good to be true, it probably is.

Cyberbullies and cyberstalkers use the social networking sites to embarrass, intimidate, or stalk someone.

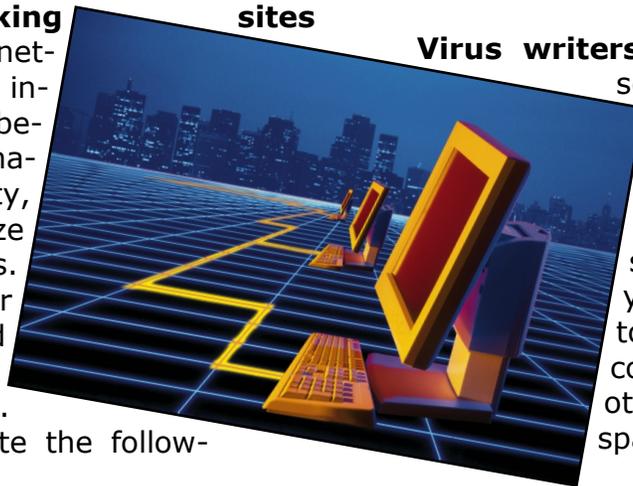
Virus writers and other scammers

send you files to download and links to malicious sites. Their goal is to infect your computer with software they can use to steal information from you. Sometimes they try to take control of your computer to use it to infect other computers or send spam to other people.

Protecting information is the key.

Below are some examples of how you can keep your information protected while using social networking sites:

- When establishing your account, adjust your profile until you are comfortable with the amount of protection provided to maximize your security.
 - Make sure your anti-virus and anti-spyware software are installed and up-to-date.
 - Choose your screen name carefully – do not include any information such as your name, age, sex, city, or employer.
 - Never post anything you would not want to have distributed publicly.
 - Never post personally identifying information such as: SSN, first and last name, address, driver's license, telephone number and e-mail address.
- Be careful posting any pictures; they can be altered and re-posted anywhere on the Internet.
- Don't click on any links or open files that can be downloaded.
- Monitor your children's activities online; teach them to protect their information.



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://>

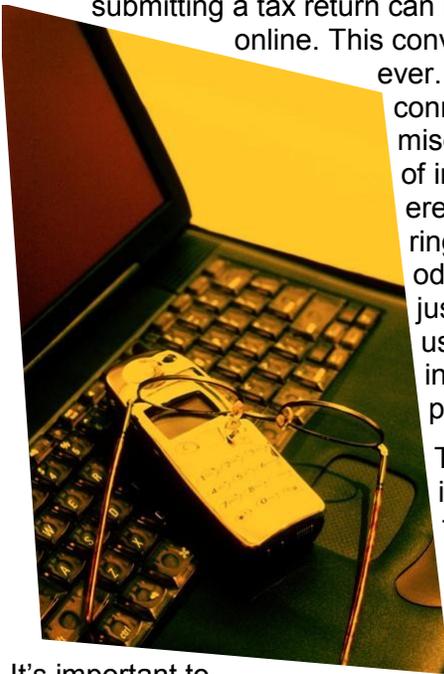
www.nationalterroralert.com/

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

Why Is Information Security Important?

Security the Information in order to use it

Many of our critical government services rely on the Internet and technology to function. Everything from renewing a driver's license online to submitting a tax return can be done quickly and conveniently online. This convenience does come with risks, however.



The average unprotected computer connected to the Internet can be compromised in less than a minute. Thousands of infected web pages are being discovered every day. Data breaches are occurring all too often. New cyber attack methods are launched continually. These are just a few examples of the threats facing us, and they highlight the importance of information security as a proactive approach to protecting data and systems.

These rapidly accelerating and increasingly sophisticated cyber threats and the potential devastating consequences they pose to our interconnected state and local governments make it clear that we must act now.

It's important to note that information security is not a technology issue, but rather a management issue requiring leadership, expertise, accountability, due diligence and risk management. Information security needs to be addressed in a coordinated, enterprise approach, and factored into program decisions.

There are three core principles of information security – **Confidentiality, Integrity, and Availability.**

Confidentiality

Confidentiality is considered the condition when designated information collected for approved purposes is not disseminated beyond a community of authorized recipients. It is a fundamental responsibility of government officials to ensure that the necessary safeguards are in place to protect information entrusted to them.

The public expects nothing less. Only

authorized personnel should have access to confidential information under the stewardship of government entities. Rights assigned to personnel who administer applications and systems must be tightly controlled and limited to the minimum levels necessary to perform their jobs. Pro-

tection of the confidentiality of information is not limited to controlling access to systems, but also applies to having appropriate safeguards in place while information is stored and being



Internet Safe Kids Pledge



I will be aware of who I talk to on the Internet.

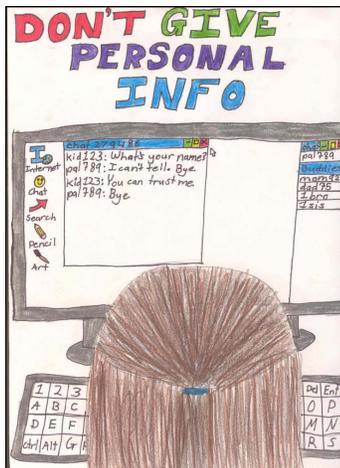
I will always block cyberbullies and always tell a trusted adult about someone cyberbullying me.



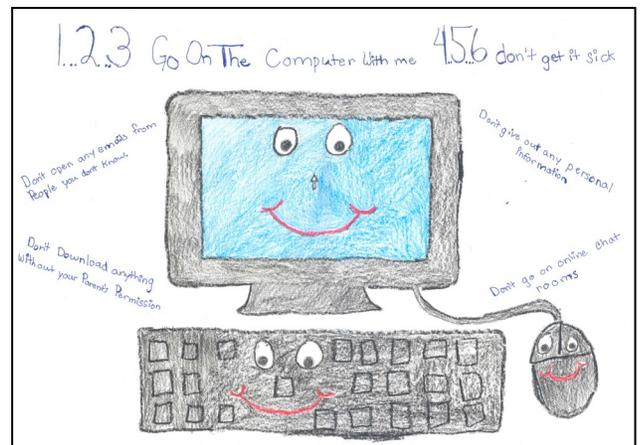
I will never agree to meet in person with a stranger that I met on the Internet.

I will never give out personal information about myself such as name, address, telephone number, my school. Neither will I post pictures of myself on-line.

I will let my parent(s) or guardian know if I receive messages that make feel uncomfortable.



I pledge that I will abide by this INTERNET SAFE KIDS PROMISE!



Signed _____ Date _____
(Student Signature)

Signed _____ Date _____
(Parent/Guardian/Educator Signature)

Why Is Information Security Important? (continued from page 4)

transported, either electronically over a network or physically transported via tapes and mobile devices such as laptops and hand-held devices.

Some examples where confidentiality is important include medical records, confidential emails, and records containing social security numbers or credit card information and personal income tax returns.

Integrity

Integrity of information is vital to instilling trust in people who use or rely on the information. Decisions impacting the health, safety and welfare of the public are made based on the assumption that the information used is accurate and reliable. Access to information must be managed so that it cannot be accidentally or maliciously altered. Controls need to be in place regarding the creation, modification and updating of information.



Availability

Availability means an information system or service is available and functioning correctly and providing information when needed by authorized users. All aspects of the service delivery should be protected in order for the service to function properly. Appropriate backup and disaster recovery strategies should be developed for every critical system or service.

Some examples where the loss of availability would impact government services include checking driving records during a traffic stop, processing finger prints of suspects, processing credit card transactions and loss of communications during a crisis or incident.



What Can You Do?

While one hundred percent security does not exist, there are steps that can be taken to manage the risks and apply due diligence in protecting information and systems.

First and foremost embrace information security as a priority. Be a champion for the cause.

Second, designate someone to be in charge of information security, as your Information Security Officer. This individual should be someone with a senior authority level, who has a “voice at the table” regarding information security aspects of the organization’s programs, policies and any new initiatives.

Third, develop appropriate policies and procedures to safeguard the information.

Fourth, empower the Information Security Officer to oversee the implementation of and compliance with the information security policies.

Fifth, train all staff. Ensure that all staff is trained periodically on your policies and best practices for protecting information. Ensure that technical staff has the appropriate training to implement and manage sound information security practices.

Avoid Phishing Scams



HELPFUL TIPS

- Do not click on any links listed in an email message and do not open any attachments from untrusted sources
- Do not enter personal information in a pop-up screen
- If it appears to be a phishing email, simply delete it
- Enable/install a phishing filter on your web browser
- Do not respond to emails asking for personal information. Legitimate organizations will not ask you to provide personal information via email

Keep Sensitive Data Secure



HELPFUL TIPS

- Keep your operating system up-to-date
- Install and update anti-virus protection software and firewalls
- Use strong passwords
- Know where sensitive information is stored on your computer
- Limit physical access to your computer
- Do not share your password
- At work, follow your organization's security policy

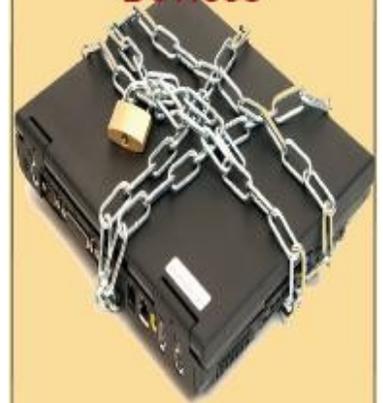
Dispose of Information Properly



HELPFUL TIPS

- Destroy/shred hard copy confidential documents that contain personal information such as social security numbers, credit card numbers, bank account numbers, health records, etc.
- Ensure you are using the right tools when destroying and disposing personal information or media storage from your computer, cd/dvd or mobile devices
- At work, follow your organization's retention and disposal procedures

Protect Portable Devices



HELPFUL TIPS

- Always keep portable devices with you when traveling
- Password-protect and lock your portable device
- Record identifying information (i.e., serial number) and label your equipment
- Keep the portable device out of sight when not in use
- Consider storing important data separately
- Report lost or stolen devices to your local law enforcement