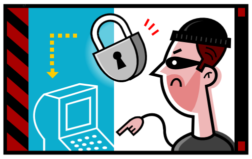


## *Don't let a Cyber Thief 'Trick' you into revealing sensitive data*

- Metro's chief information officer, **Elizabeth Bennett**, has compiled this comprehensive report on the importance of cyber security at the workplace and at home.

October is National Cyber Security Awareness Month, and for good reason. It seems that on a daily basis, we hear reports of companies having suffered data breaches. Cyber thieves always seem to find a new way to hack, connive, or steal financial and sensitive data (like payment cards and personal information) from large and small companies.

Cyber security is our shared responsibility. No one individual is solely responsible for securing Metro's Internet and Intranet resources. Everyone at Metro has a role in securing the computers, data and networks we all use. Our individual actions impact our cyber security and how we protect our technology and data.

## *Recent Cyber Security Breaches:*

### September 21, 2010

Hackers exploited a security flaw on the popular micro-blogging site Twitter. The Twitter website is being widely exploited by users who have stumbled across a flaw which allows messages to pop-up and third-party websites to open in your browser just by moving your mouse over a link, even exposing users to unwanted adult sites.

### September 09, 2010

The Walt Disney Co. acknowledged on Thursday, that it has been hit by a spate of spammed emails containing a virus, which reportedly has hit other firms as well. A Disney spokesman said the spams started flowing into company email boxes Thursday afternoon but did not affect business operations. The entertainment-business site TheWrap.com reported that Disney, Coca-Cola Co. and Google Inc. were all blasted by the spams, which include a file featuring the phrase "**Here You Have**" in the subject line.

### Understanding Cyber Security

## *Identity Theft and Identity Fraud*

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. There are currently excellent state resources and laws that protect us from the Internet jungle! Check this site often for their "Privacy tip of the Month"

***http://www.privacy.ca.gov/***

## *Data Breach*

*A data breach is the unintentional release of personally identifiable information (PII) and other forms of secure information to untrusted people and places. How widespread is this issue? As of August, 2010, the most recent total from the Privacy Rights Clearinghouse shows more than a* ***half billion*** *sensitive records breached since 2005, leaving Americans vulnerable to identity theft.* Employees losing laptop computers, hackers downloading credit card numbers and sensitive personal data accidentally exposed online -- the Chronology of Data Breaches shows hundreds of ways that the personal information of consumers is lost, stolen or exposed.

The Chronology of Data Breaches, a project of the Privacy Rights Clearinghouse since 2005, lists incidents involving breached consumer information, such as personal medical records, credit card numbers and Social Security numbers. The most recent total, published August 24, 2010, is a wake-up call to consumers who think identity theft can't happen to them.

***http://www.privacyrights.org/data-breach***

### Protect your data and computer system

**"Safety First"** is the motto at Metro. This should also be philosophy of Metro employees and their families while engaged in home computing activities:

1. **Shopping on the internet**:

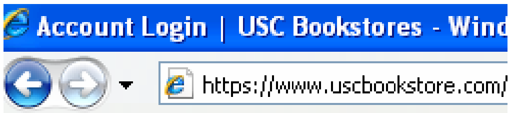
Here are some excellent Safe Internet Shopping tips from The Privacy Rights Clearinghouse which is a nonprofit consumer organization, established in 1992 and located in San Diego.

***http://www.privacyrights.org/fs/fs23-shopping.htm***

- What is a Secure Website and why do we care?

  Safe Internet shopping means a secure Web site. It uses encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your personal information as well as your credit or debit card number. This prevents computer hackers, "bad guys" from obtaining it en route. The only people who can unscramble the code are those with legitimate access privileges, the "good guys". Unfortunately you can't tell who is who by the colors of their hats! But you can tell if you are dealing with a secure Web site in several ways:

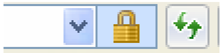
- First, if you look at the top of your screen where the Web site address is displayed, you should see **https://**. The "**s**" that is displayed after "http" indicates that Web site is secure. Often, you do not see the "s" until you actually move to the order page on the Web site.



Account Login | USC Bookstores - Wind

https://www.uscbookstore.com/

- Another way to determine if a Web site is secure is to look for a closed padlock usually displayed at the top right side or at the bottom of your screen.



- Do business with companies you already know. Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line. If the company is unfamiliar, call them and ask about their return and refund policies. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy.

## 2. On the Web, Children Face Intensive Tracking

“Big Brother” is on your computer. A Wall Street Journal investigation into online privacy has found that popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults. 50 sites popular with U.S. teens and children were examined to see what tracking tools were installed on a test computer. As a group, the sites placed 4,123 "cookies," "beacons" and other pieces of tracking technology. The tiny tracking tools (software programs) are installed on a computer when a user visits some Web pages. They are used by data-collection companies to follow people as they surf the Internet and to build profiles detailing their online activities, which advertisers and others buy. The profiles don't include names, but can include age, hobbies, shopping habits, race, and general location information, such as city.

Parents should remind children — younger kids in particular — not to give out their name, phone numbers, or other personal information online.

Learn more at ***http://www.staysafeonline.org/***

## 3. *Social Networking Privacy: How to be Safe, Secure and Social*

While websites like Facebook and MySpace make it easy to share vacation photos with old classmates, the personal information on social networks is also attracting people besides friends and family members. Scam artists, identity thieves, debt collectors, stalkers, hiring managers, and companies looking for a marketing advantage are turning to social networking sites to gather valuable information. Before you publish your next status update, take care that you aren’t risking your identity, security or reputation.

Below are some things you *shouldn’t* give to a social network – when signing up for an account, posting content or interacting with your contacts through the network.

a) Access to your email account. During the registration process, social networks often solicit a new user to provide an email address and account password so they can access the user’s email address book. To be safe, don’t provide this information at all. ***Use privacy settings to restrict it to approved contacts***

b) Never provide a work-associated email to a social network, especially when signing up. Consider creating a new email address strictly to connect with your social networking profile(s).

c) Vacation Plans. Don’t publicize vacation plans, especially the dates you’ll be traveling.

d) Compromising, sensitive, embarrassing or inflammatory pictures or posts. Remember that whatever goes on a network might eventually be seen by people not in the intended audience. Think about whether you would want a stranger, an insurance agent, the government, your mother or a potential boss to see certain information or pictures. Don’t be afraid to ask to have content removed. Read more about this at ***http://www.privacyrights.org/social-networking-privacy***

e) Money. Be wary of requests for money, even if they are from contacts you know and trust. If a contact's account is compromised, a scam artist may use his or her name and account to attempt to defraud others through bogus money requests.

Remember, the strongest tools users have to defend their personal privacy on social networking sites are *common sense, caution and skepticism.*

Learn more about social networking privacy – by reading PRC's newest fact sheet

**[http://www.privacyrights.org/fs/fs18-cyb.htm#cookies](http://www.privacyrights.org/fs/fs18-cyb.htm#cookies)**

### 4. *Tips for Keeping Your Computer Secure*

**[http://www.privacyrights.org/fs/fs18-cyb.htm#secure](http://www.privacyrights.org/fs/fs18-cyb.htm#secure)**

**Personal Computer Security: Using Uncommon Sense | ZDNet**

This article explains in a humorous manner the sometimes confusing terms like; anti-virus and anti-malware, ad blockers, social engineering, network addressing, as well as hardware and software firewalls. It has links to free tools (like antivirus) for home computing protection.

**[http://www.zdnet.com/blog/perlow/personal-computer-security-using-uncommon-sense/13878?tag=nl.e539](http://www.zdnet.com/blog/perlow/personal-computer-security-using-uncommon-sense/13878?tag=nl.e539)**

## *To sum it up:*

Watch what you share and with whom.

Never click on links in emails from unknown persons.

Never answer an email from a bank or institution wanting to "update" your personal and financial information

Consider your identity information as currency. Spend it wisely.

To keep you and your family cyber secure, be safe, be careful, and be attentive.