

Best Practices for Secure Computing at Westminster

Last Updated: 10 March 2006

Information Technology Department

1. Creating Secure Passwords

Do not share your Westminster computer user account password(s) with anyone. *Users of the administrative database (Athena, Colleague, Benefactor) contact IT for password info.*

- Your password must be at least **six** characters long with no spaces or quotes. Do not use birthdates, phone numbers, family or pet names, or any part of your username.
- The strongest passwords use a combination of MiXed caSe letters, numbers, and symbols:
 - T@nsTa@fL! (There ain't no such thing as a free lunch)
 - Iam#3oF5 (I am the third of five children)

2. Securing Your Workstation

When you log in to your Westminster account, the computer you are at has access to all of your files, network access privileges, email, employee information, and more — **and so does anyone using that computer while you are logged in.**

- Always log off when you are finished using a computer by clicking Start > Log Off.
- If you need to leave your workstation for a moment, lock it by using Windows Key + L.

3. Protecting Yourself from Identity Theft

Identity theft is a 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. Further information is available at <http://www.usdoj.gov/criminal/fraud/idtheft.html>

4. Email and Security

You must assess each email individually to decide if it is legitimate; you cannot rely on the displayed sender address. It is easy to fake legitimate email addresses. If in doubt, call the author and verify it. See the examples emails attached to this document.

- Do not send email containing confidential information.
- Do not respond to emails asking you to provide confidential information (usually by following a hyperlink to a web page with a form, or by filling out a form in the email).
- Assume every attachment contains a virus, whether or not you know the sender. Before you open attachments, save them to your desktop and scan them for viruses, then move them to your H: drive.
- Do not reply to or follow “unsubscribe” links in suspicious emails.
- Use your email system's Junk Mail handling tools to block spam and unwanted email.

5. Avoiding Computer Viruses and Spyware/Adware

Computer viruses are malicious programs that intentionally cause computing problems. Spyware and adware are subtle programs that typically harvest user information, secretly reporting the websites you browse or creating popup windows. To avoid viruses, spyware and adware:

- Do not install free entertainment software such as games, screen savers, graphic themes, and music- or file-sharing utilities; such software often contains hidden viruses or spyware.
- Be alert while browsing websites. **Pay attention to where you click and read screens.** Do not install software from websites unless you need it and are certain of what it does.

Parts of this document were adapted from the following sources:

http://www.ncjrs.org/spotlight/identity_theft/summary.html

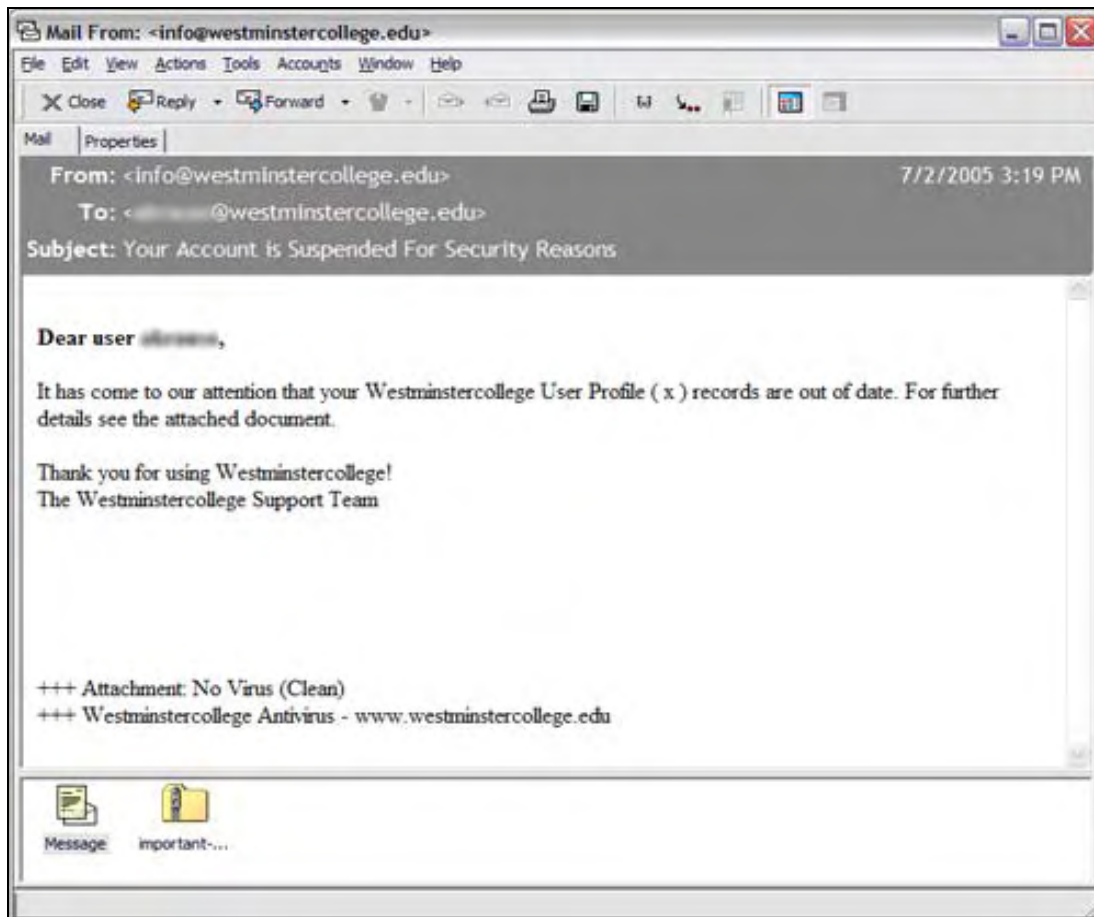
<http://www.it.utah.edu/leadership/security/identity.html>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

http://www.antiphishing.org/phishing_archive

Example 1: Spoof Email with Virus Attachment

This email author has used the recipient's email prefix and, correctly, guessed our convention for usernames. It spoofs what appears to be an administrative Westminster email account and directs the recipient to open the attachment (which is a virus). Note that the author has added fictitious "virus scan" text at the bottom as if it was scanned by anti-virus software.



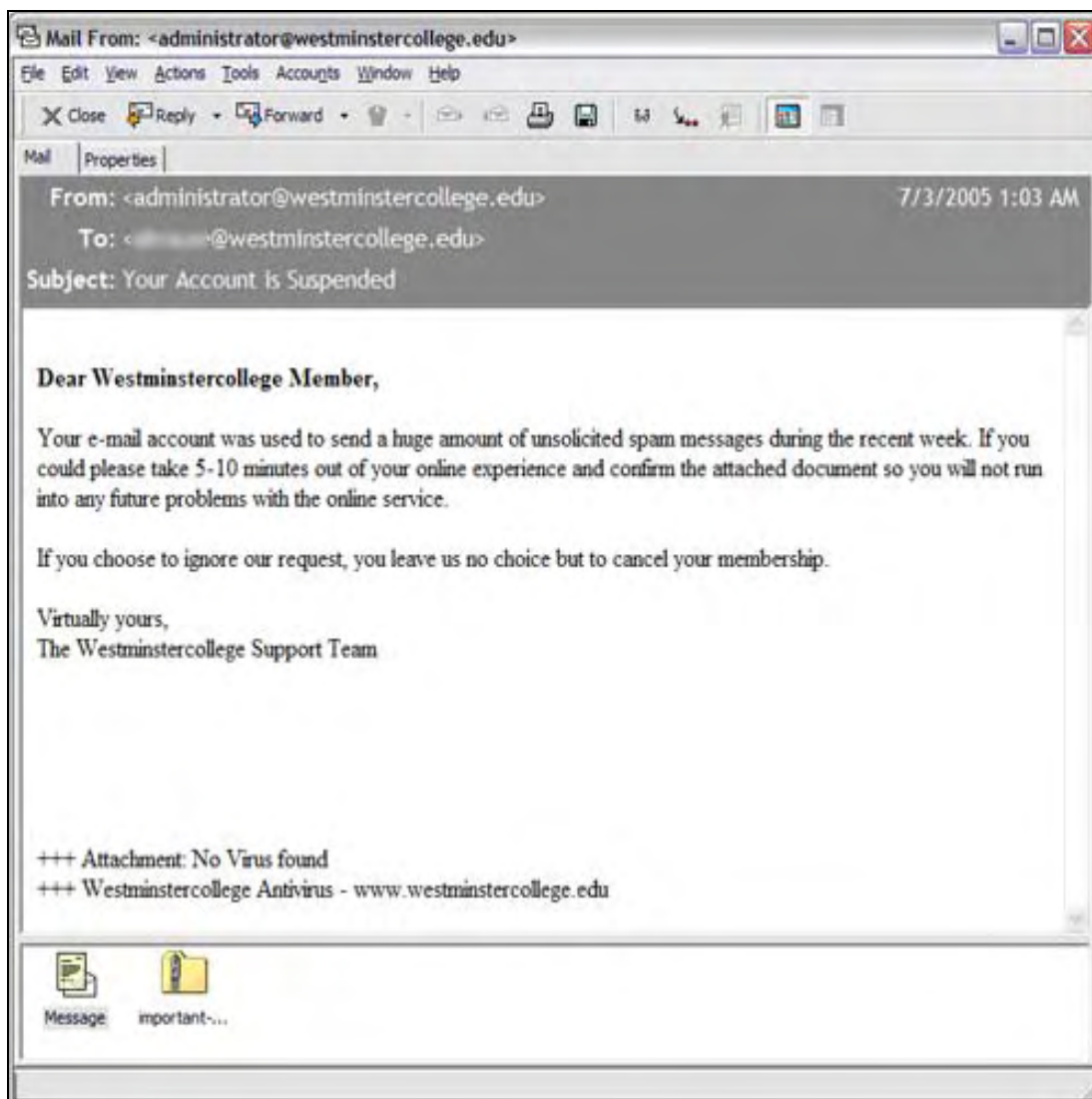
Parts of this document were adapted from the following sources:

http://www.ncjrs.org/spotlight/identity_theft/summary.html
<http://www.it.utah.edu/leadership/security/identity.html>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>
http://www.antiphishing.org/phishing_archive

Example 2: Spoof “Administrator” Email with Virus

This email relies on some clever writing and social engineering to fool the reader. The author has spoofed what appears to be a legitimate Westminster email address. The email reads like boilerplate notification text an IT department would send and prompts the user to open the attachment (a virus) or threatens to “cancel their membership.” This email also contains fictitious text implying that it has been scanned and is free of viruses.



Parts of this document were adapted from the following sources:

http://www.ncjrs.org/spotlight/identity_theft/summary.html
<http://www.it.utah.edu/leadership/security/identity.html>

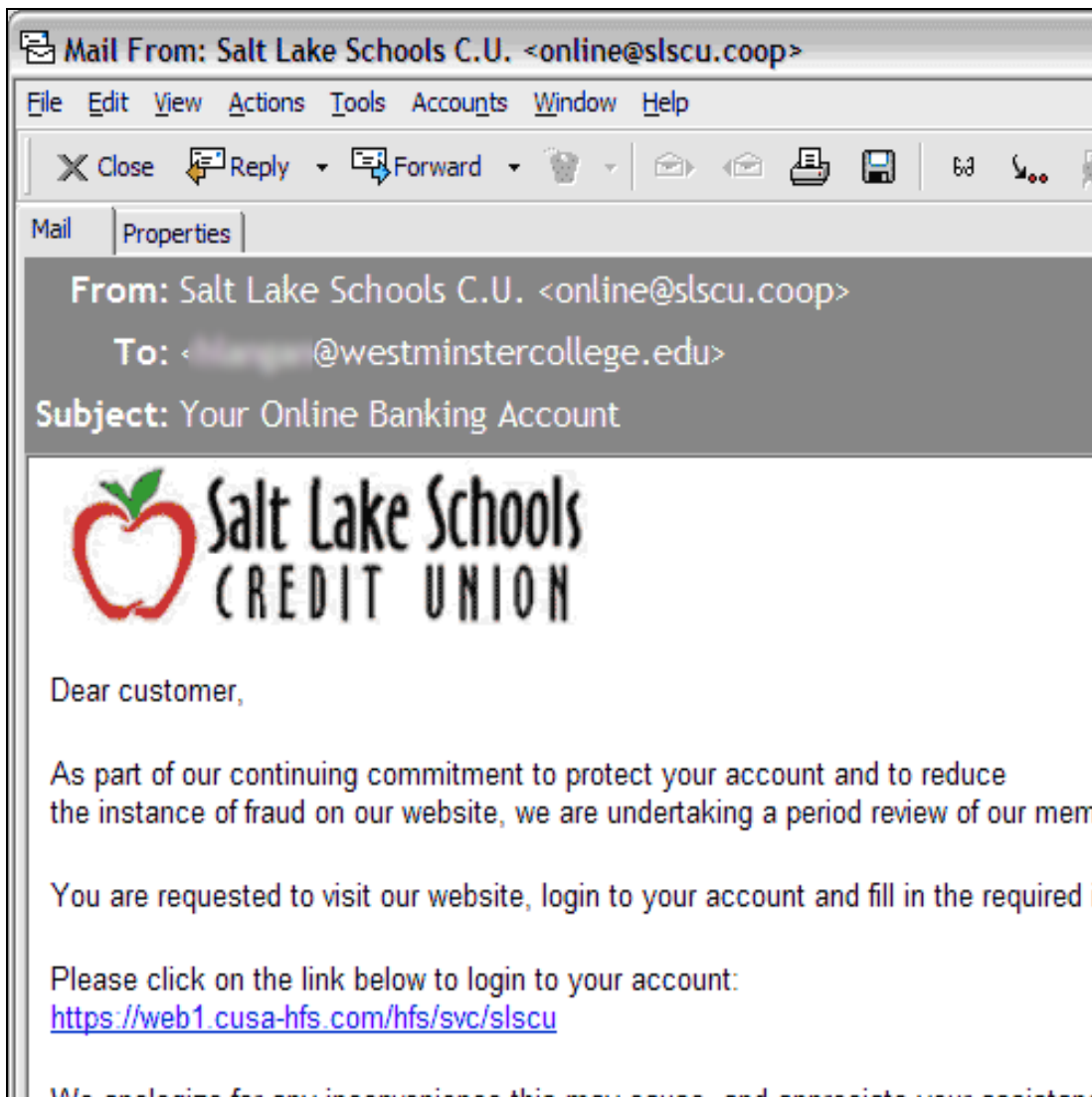
<http://www.usdoj.gov/criminal/fraud/idtheft.html>
http://www.antiphishing.org/phishing_archive

Example 3: Phishing Email Linking to Fraudulent Website

This kind of email appears to be legitimate, official correspondence from a bank. It uses a graphic (probably taken from the bank’s website) and is fairly well written. It may even be using the name of a legitimate banking authority (again, probably taken from the bank’s website).

The hyperlinked text appears to go to the actual website, but clicking on it takes users to a fake website to harvest confidential info. Linked text has nothing to do with the actual hyperlink address: you could link the words “free DVD player” and take users to the Westminster website.

- To access confidential information on a website or to conduct legitimate online transactions, use a secure browser and type the correct website address directly. Don’t follow hyperlinks sent to you via email. You should always ensure you have a secure connection, typically indicated by “https” at the beginning of the website address.



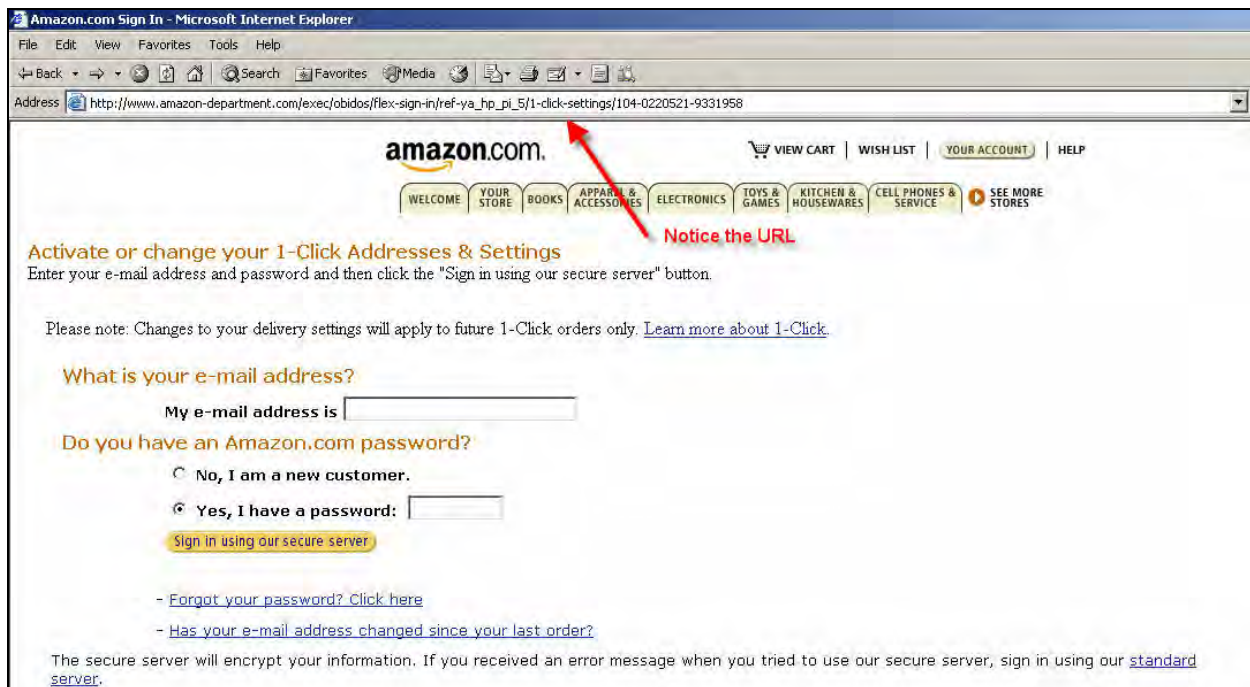
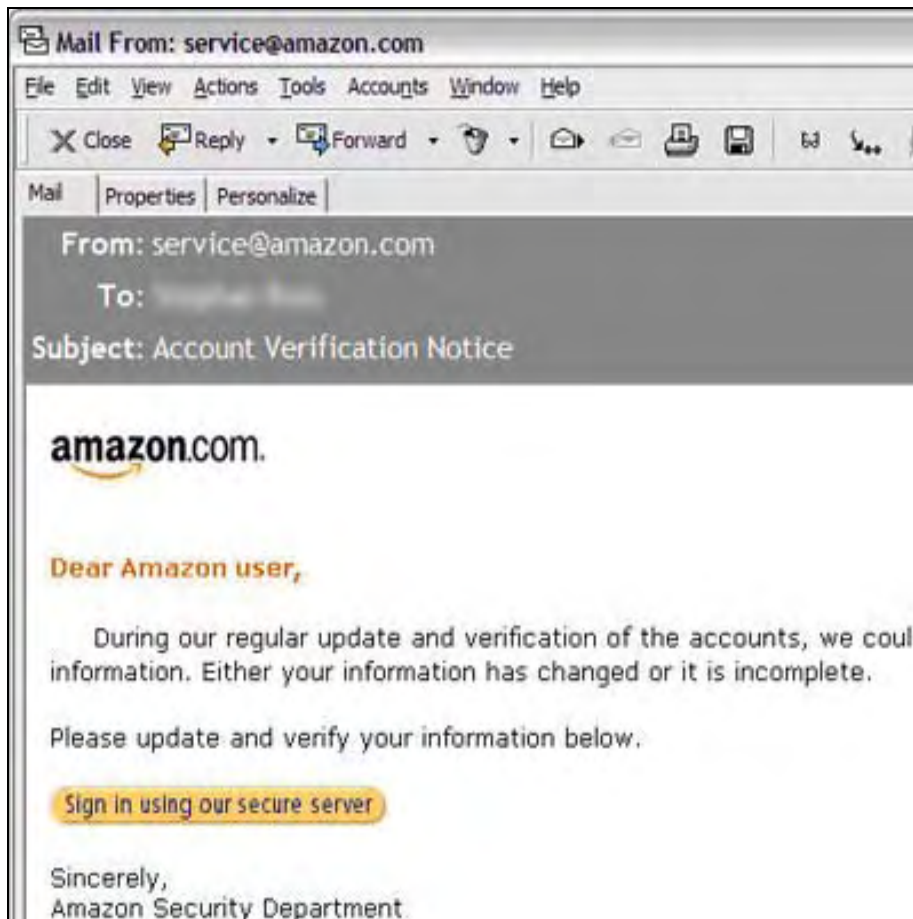
Parts of this document were adapted from the following sources:

http://www.ncjrs.org/spotlight/identity_theft/summary.html
<http://www.it.utah.edu/leadership/security/identity.html>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>
http://www.antiphishing.org/phishing_archive

Example 4: Phishing Email Mimicking a Web Page

This email and its fraudulent website mimic the look of a vendor's website. Notice that the URL is not that of the vendor. After filling out the "phishing" form, users are sent to the real vendor website.



Parts of this document were adapted from the following sources:

http://www.ncjrs.org/spotlight/identity_theft/summary.html

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

<http://www.it.utah.edu/leadership/security/identity.html>

http://www.antiphishing.org/phishing_archive