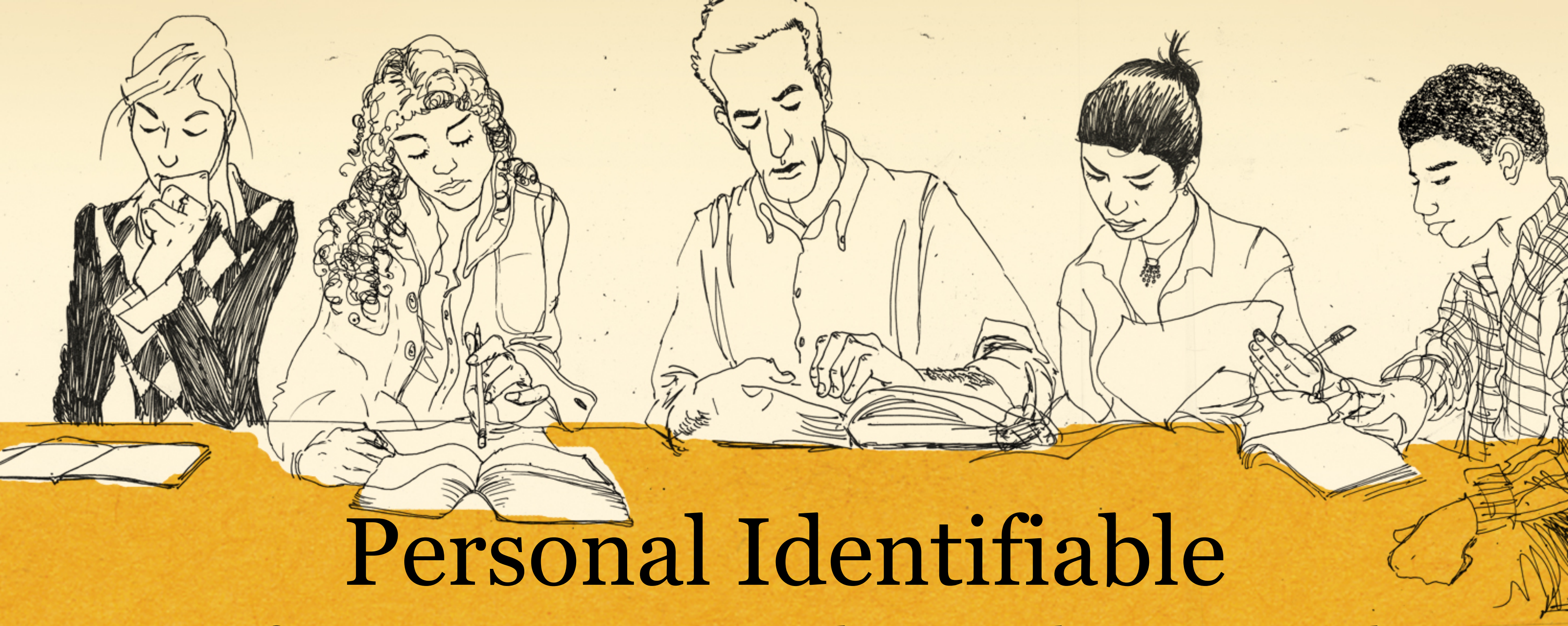


Personal Identifiable Information and Dealing with Scams/Phishing

Salt Lake Community College

Step Ahead.

Training Goals

- The purpose of today's training is to introduce you to SLCC's policies on how to store personally identifiable information (PII)
- How to avoid online scams.

Terms

- **PII-Personally Identifiable Information:** is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

- Examples:
- Social Security Numbers
- Credit Card Numbers
- Driver's License Numbers

Salt Lake Community College

PII Storage 101

- Do not store PII on C:\ drives, thumb/flash drives or other portable devices.
- When you need to save documents that contain PII save them to the H drive or I drive. If you need to access the documents offsite, you can connect using the VPN and map your H drive and I drive.

Salt Lake Community College

PII 101

- Do not e-mail PII to others in the College or to outside organizations.
- If the documents are needed to be shared inside or outside the College, the Information Security Office can assist with a secure way to transmit the documents.
- Credit Card Numbers should never be stored in clear text. **The numbers must be encrypted**. This is due to Payment Card Industry (PCI) regulations.

Salt Lake Community College

PII

- Information Security will be doing scans for PII and will work with departmental supervisors to remediate the files.
- Example of output from the scan
- "Determine if a file contains a valid VISA credit card number." : [FAILED] Share: C$, path: \documents and settings*******\my documents \forms\word\toner order form.dotx (XXXXXXXXXXXX4011)

Salt Lake Community College

FERPA

- Family Educational Rights and Privacy Act

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

FERPA Training

- For more information on FERPA contact Enrollment Services for training information.
- Patricia Sanchez 957-4296
- MaryEtta Chase 957-4799

Payment Card Industry(PCI)

In order for SLCC to use credit cards we must comply with the PCI standards.

These rules govern how we can transmit, store and process credit cards.

Salt Lake Community College

Terms

- **Phishing**: a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to *Fishing*, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.
- **Spear Phishing**: Targeted Phishing attack.
- **Phone Phishing**: A phishing attacked over the phone
- Source Wikipedia

Salt Lake Community College

Security 101

- Lock your computer when you are away from it by pressing Windows key and L.
- Back up all important data to the H drive or I drive. (OIT backs ups these drives.)
- Do not store sensitive information on C drive, thumb drives or other portable devices.

Salt Lake Community College

Security 101

- Do not give your password to others. This includes long distance call out codes.
- Do not write your password down and leave it near your computer. This includes your long distance call out code.
- If you are unsure about an attachment do not open it and report it to the Help Desk.
- Remember email is like a post card. Do not put information in an email that you would not write on a post card.

Salt Lake Community College

Security 101

- If your Laptop is stolen report it to Campus Police and your supervisor.
- OIT will NEVER ask for your password.

Salt Lake Community College

Avoid Phishing

- Never give out personal or financial information. (This includes following/clicking links sent in the email.)
- Do your best to verify website security:
  - Inspect the URL of a web site.
  - Bookmark all sites you do business with.
  - Bogus sites may appear almost identical to the original
  - Be aware of domain usage (.com versus .net, etc.)
  - Beware of Tax Season IRS scams.
  - Beware of Mortgage Relief Scams.

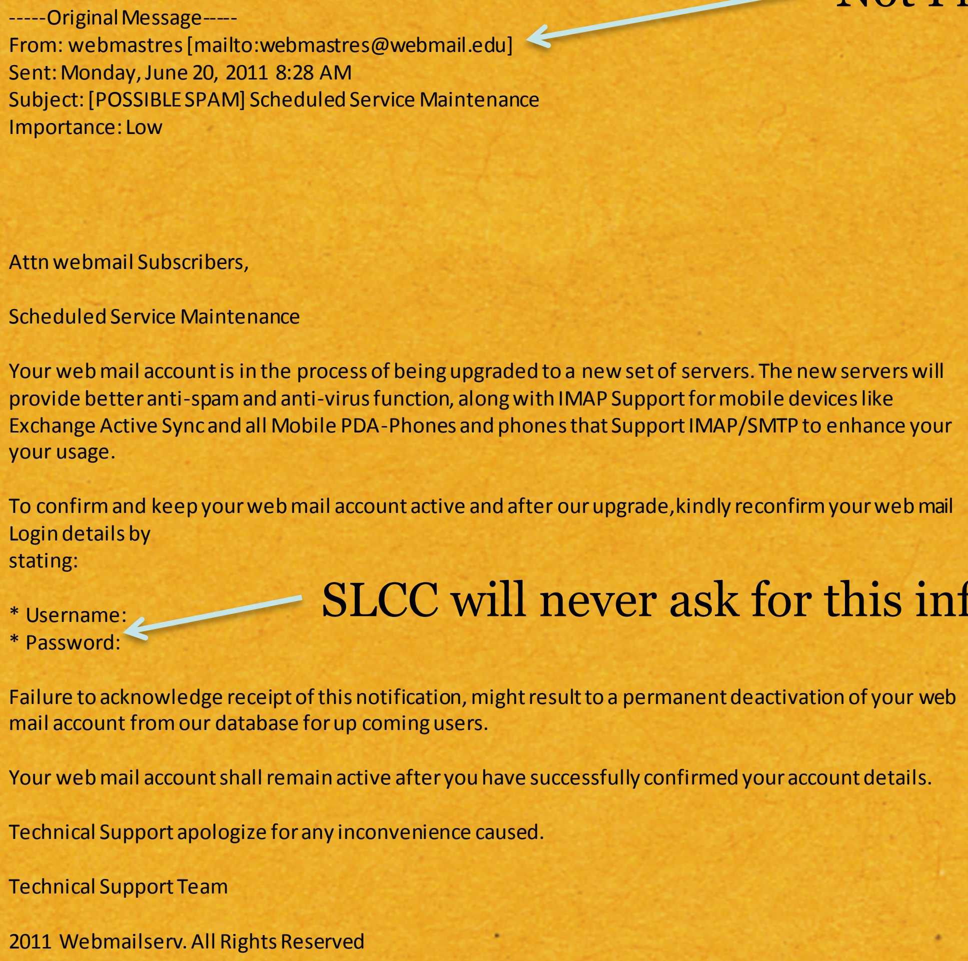
Salt Lake Community College

Avoid Phishing

- If you are unsure whether an email request is legitimate, try to verify it by contacting the company\agency directly. Do not use any contact information from the email.

- Information about known phishing attacks is available online from groups such as the Anti-Phishing Working Group: www.antiphishing.org

Phishing E-mail



-----Original Message-----
From: webmastres [mailto:webmastres@webmail.edu]
Sent: Monday, June 20, 2011 8:28 AM
Subject: [POSSIBLE SPAM] Scheduled Service Maintenance
Importance: Low

Attn webmail Subscribers,

Scheduled Service Maintenance

Your web mail account is in the process of being upgraded to a new set of servers. The new servers will provide better anti-spam and anti-virus function, along with IMAP Support for mobile devices like Exchange Active Sync and all Mobile PDA-Phones and phones that Support IMAP/SMTP to enhance your your usage.

To confirm and keep your web mail account active and after our upgrade, kindly reconfirm your web mail Login details by
stating:

* Username:
* Password:

Failure to acknowledge receipt of this notification, might result to a permanent deactivation of your web mail account from our database for up coming users.

Your web mail account shall remain active after you have successfully confirmed your account details.

Technical Support apologize for any inconvenience caused.

Technical Support Team

2011 Webmailserv. All Rights Reserved

Not From SLCC

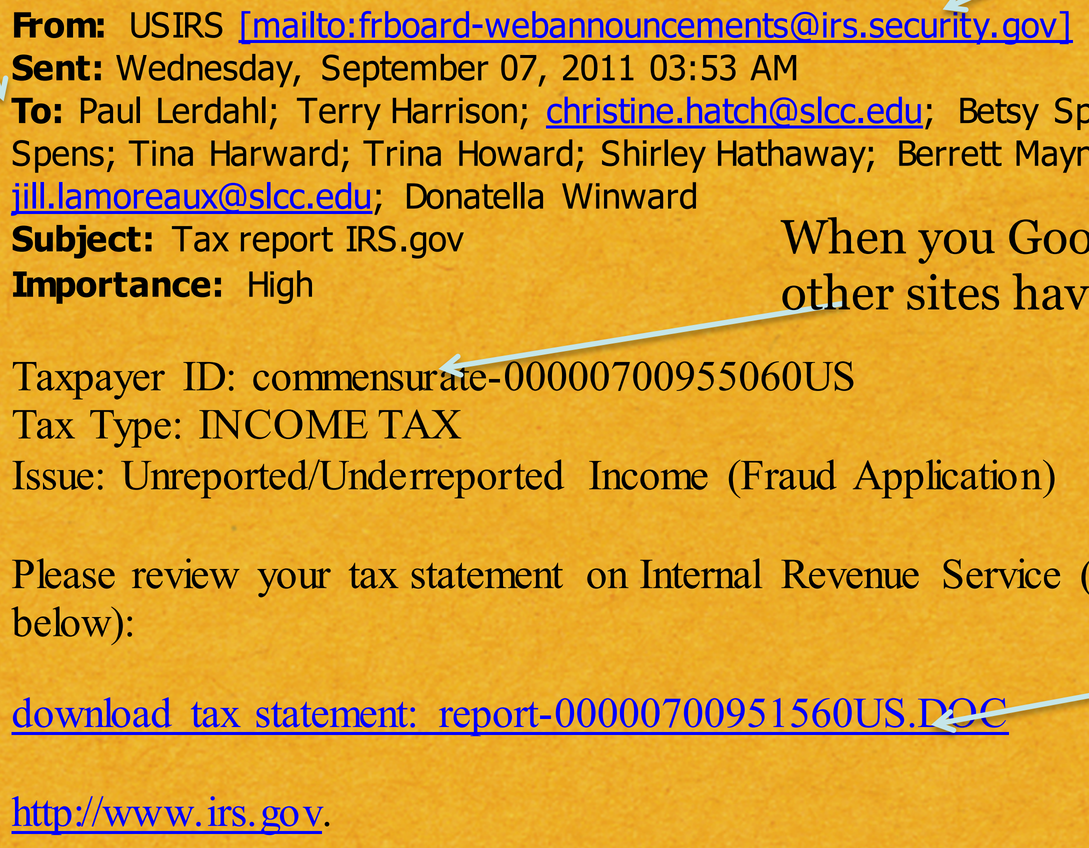
SLCC will never ask for this information in an email

Salt Lake
Community
College

Sample Phishing E-mail

To many names listed to be a real email

Wrong address for IRS



From: USIRS [mailto:frboard-webannouncements@irs.security.gov]
Sent: Wednesday, September 07, 2011 03:53 AM
To: Paul Lerdahl; Terry Harrison; christine.hatch@slcc.edu; Betsy Specketer; Georgenia Beams; Timothy Spens; Tina Harward; Trina Howard; Shirley Hathaway; Berrett Maynard; Anna Thornton; jill.lamoreaux@slcc.edu; Donatella Winward
Subject: Tax report IRS.gov
Importance: High

When you Google this line you see many other sites have listed it as a Phishing Scam

Taxpayer ID: commensurate-00000700955060US
Tax Type: INCOME TAX
Issue: Unreported/Underreported Income (Fraud Application)

Please review your tax statement on Internal Revenue Service (IRS) website (click on the link below):

download tax statement: report-00000700951560US.DOC

This is the malicious link

http://www.irs.gov.

Salt Lake Community College

Phishing E-mail

From: Isabella Charlotte [mailto:irs-irs@xixia.net]
Sent: Wednesday, March 21, 2012 10:12 PM
To: Phyllis Seyler
Subject: Re: TAX EXEMPTION NOTIFICATION

Sir/Madam,

Our records indicate that you are a Non-resident. As a result you are exempted from United States of America Tax reporting and withholdings on interest paid to you on your account and other financial benefits. To protect your exemption from tax on your account and other financial benefits, you need to recertify your exemption status and enable us confirm your records with us.
Therefore, you are to authenticate the following by completing form W-4100B2 and return to us as soon as possible through fax numbers no +1-815-390-1251
When completing form W-4100B2, please follow the steps below:

1. We need you to provide your permanent address if different from the current mailing address.

2. You must indicate as a Non-US resident, the country you are residing, to support your non-resident status and if your bank or other financial institutions you are dealing with has a US address for mailing purposes.

3. If any joint account holder is now a US resident or citizen, or in any way subject to US tax
reporting laws: please check the box in this section.

4. Please complete 1 through 19 and have all account holder/s (if more than one account holder) sign and date the form separately and fax to the above-mentioned fax numbers.
Please complete Form W-4100B2 (attached) and return to us with one week from the receipt of this letter by faxing it, to enable us confirm your records immediately. If your records are not confirmed on time, you will lose your Non-resident status tax exempt benefits and your account or any other financial benefits will be subject to US tax reporting and back up withholding*

*If back up withholding applies, we are required to withhold 30% of the interest/benefits paid to you.
We appreciate your cooperation in helping us protect your exempt status and also confirm our records.
Sincerely,
Isabella Charlotte,
IRS Public Relations

Salt Lake Community College

Phishing/Scam Phone Calls

Examples of a phishing/scam phone calls:

Some of these are””robo calls” and some are not.

You have been selected for a political survey and after completing the survey you will receive a Caribbean Cruise to the Bahamas for two paid for by one of the political backers except for taxes and port fees. After the survey the call ask for your credit card number to cover the taxes and fees.

The bait is the free cruise and the goal is to get your credit card number.

Last chance to lower your credit card interest rate. Please enter your card number to get the best rates possible.

The bait is the last chance to get a lower rate and the goal is to get your credit card number.

What if you were phished?

- Report it to the Help Desk (5555).
- If you believe your financial accounts may be compromised, contact your financial institution immediately.

What if you were phished?

- Watch for any unauthorized charges to your account.
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission or the FBI's Internet Crime Complaint Center.

Salt Lake Community College

Recognizing Scams

- OIT will **NEVER** ask for your password!
- If it sounds too good to be true, it probably is!
- If the message does not appear to be authentic, it's probably not.
- Check to see if the content of the message appears in search engine results (known scam, etc.)
- Watch for typographical errors, bad formatting, poor grammar, etc.

Salt Lake Community College

Recognizing Scams

- The message asks you to send your information to them, rather than the other way around.
- You do not have an account with the company supposedly sending the email.

- Facebook Scams: To learn about scams on Facebook follow the link.

Questions ?

- Thank you for attending
- http://cms.slcc.edu/iso
- Daniel.J.Baker@slcc.edu (x4875)
- Jason.Tracy@slcc.edu (x5022)

Salt Lake Community College