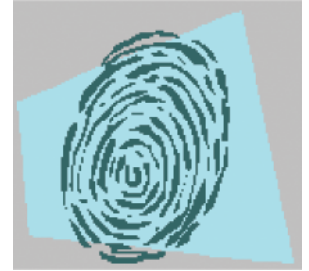


Identity Theft



1. Information Security Updates
2. Presentation
3. Question and Answer Period

Vicki Stover, Ryan Matteson
Thursday, July 26, 2007
University Union, Room 220



1. Have you had **your** identity stolen?
2. Can you reduce the chance of identity theft?
3. How?

Identity Theft

“Identity theft is the fastest growing crime in America, with 9.9 million victims reported last year” - *FTC*

What is identity theft?

- Legal definition:
“Fraud related to activity in connection with identification documents, authentication features, and information”

What is identity theft?

Low Risk

+ High Reward

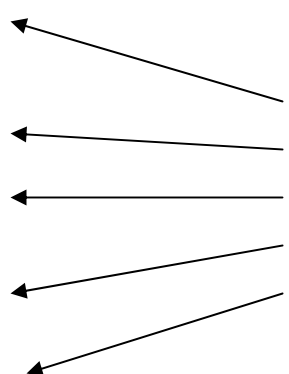
+ Opportunity

= Criminal's Dream

What is *your* identity?

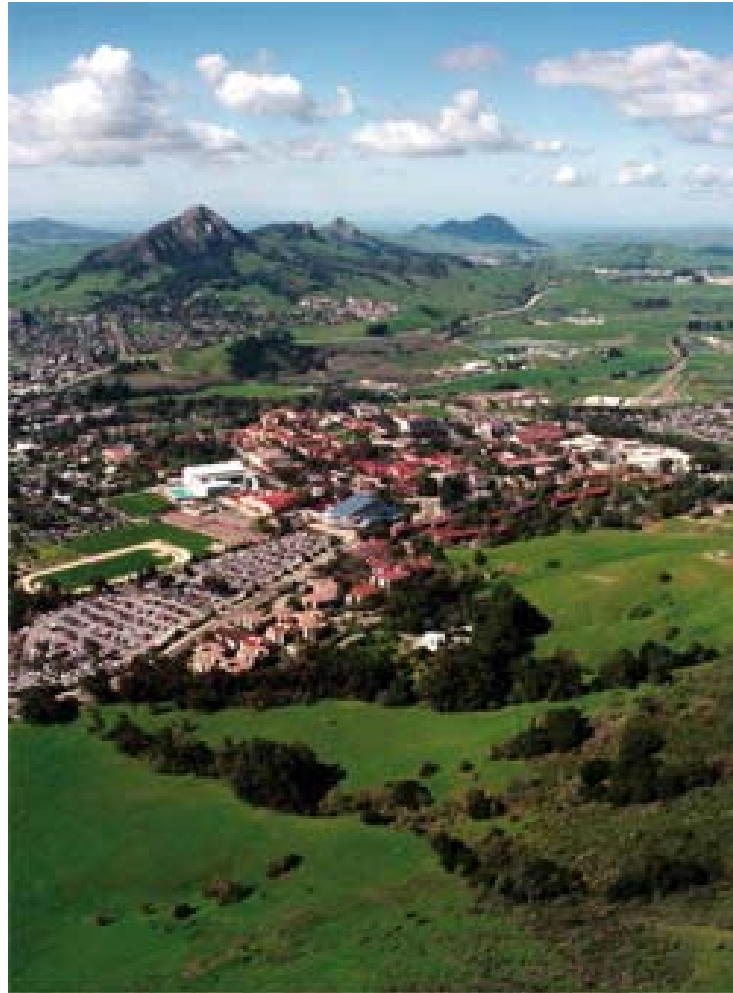
- Powerful information:
 - credit card accounts
 - bank accounts
 - passwords and PINs
 - SSN
 - driver's license

What is *your* identity?

- Powerful information:
 - credit card accounts
 - bank accounts
 - passwords and PINs
 - **SSN**
 - driver's license
- Allows**
“them”
to act as
“you”
- 

- Scary: Existing Accounts
- **Really Scary: *New* Accounts**

We Live in a Nice Neighborhood



We Live in a Dangerous Neighborhood



Who perpetrates this fraud?

- Anyone who has or can get access to your information:
 - Insiders (local, or not)
 - Dumpster divers, burglars, pick pockets, etc. (local, or not)
 - Criminal underground on the Internet
- Out to get someone...

How they do it...

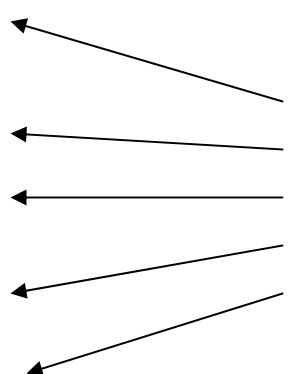
- Phishing
- Viruses/Worms/Trojans - Botnets
- 95% of email is SPAM

A blessing and curse...



1. Don't buy a computer
2. If you must buy a computer, don't turn it on.
-- Jeff Richards' Laws of Data Security

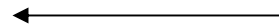
What is *your* identity?

- Powerful information:
 - credit card accounts
 - bank accounts
 - passwords and PINs
 - **SSN**
 - driver's license
- Allows**
“them”
to act as
“you”
- 

- Scary: Existing Accounts
- **Really Scary: *New* Accounts**

What is *your* identity?

- Powerful information:
 - credit card accounts
 - bank accounts
 - passwords and PINs
 - **SSN**
 - driver's license



Allows
“them”
to act as
“you”

- Scary: Existing Accounts
- **Really Scary: New Accounts**

Action you should take...

Phish or no phish? Let's practice...

<http://www.sonicwall.com/phishing/>

Check for cpSPAM

- Not a guarantee, but a useful hint...
- Consider using a filter

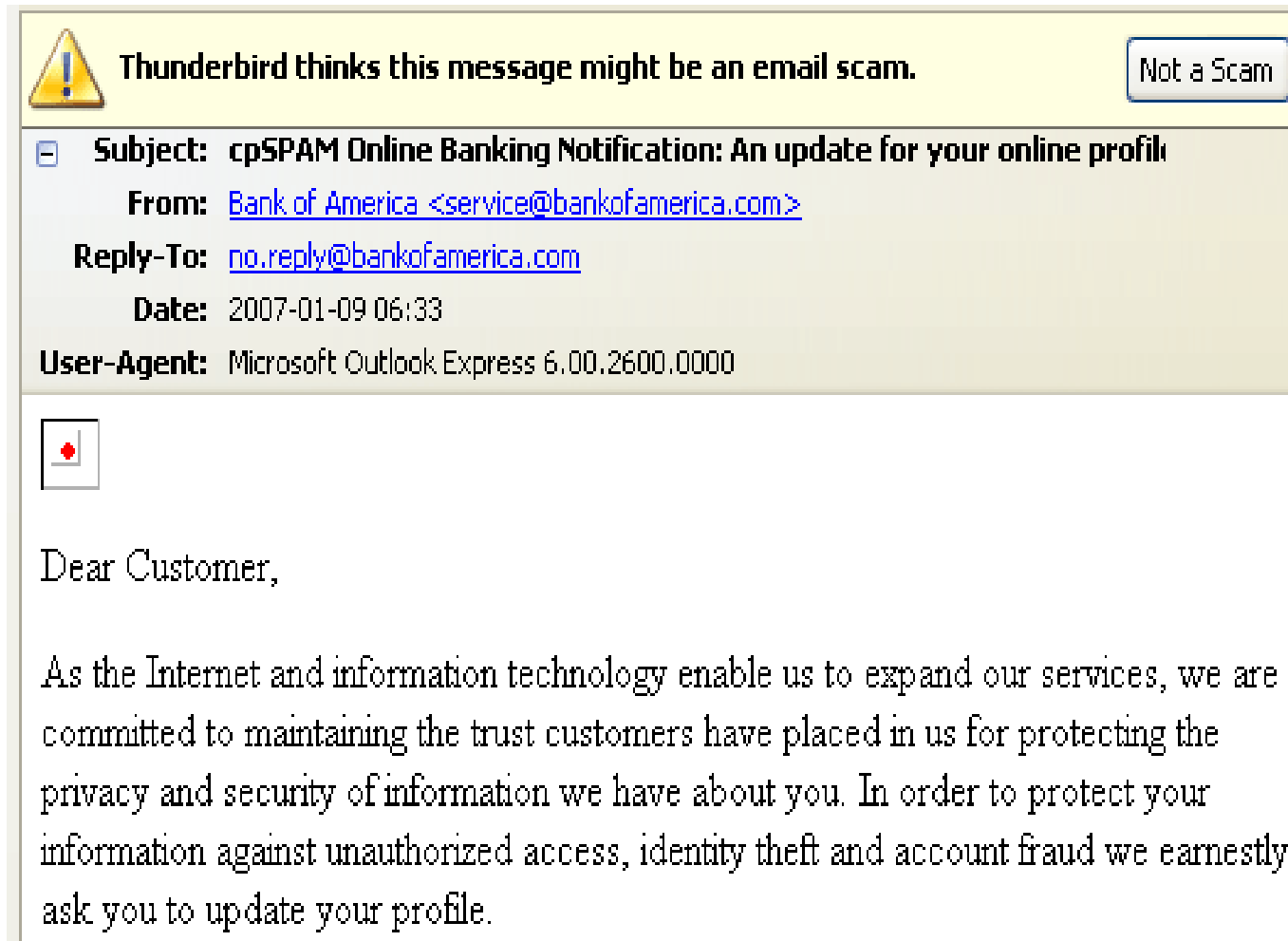
 Subject: cpSPAM Online Banking Notification: An update for your online profil
From: [Bank of America <service@bankofamerica.com>](mailto:service@bankofamerica.com)
Reply-To: no.reply@bankofamerica.com
Date: 2007-01-09 06:33
User-Agent: Microsoft Outlook Express 6.00.2600.0000



Dear Customer,

As the Internet and information technology enable us to expand our services, we are committed to maintaining the trust customers have placed in us for protecting the privacy and security of information we have about you. In order to protect your information against unauthorized access, identity theft and account fraud we earnestly ask you to update your profile.


Your email client may help...



The screenshot shows an email client interface with a yellow warning banner at the top. The banner contains a warning icon (a triangle with an exclamation mark) and the text "Thunderbird thinks this message might be an email scam." To the right of the banner is a button labeled "Not a Scam". Below the banner, the email header is displayed, including the subject, from, reply-to, date, and user-agent. A red arrow points from the left side of the slide to the warning banner. The email body begins with a red cross icon and the text "Dear Customer," followed by a paragraph of text.

Thunderbird thinks this message might be an email scam. Not a Scam

Subject: cpSPAM Online Banking Notification: An update for your online profil
From: [Bank of America <service@bankofamerica.com>](mailto:service@bankofamerica.com)
Reply-To: no.reply@bankofamerica.com
Date: 2007-01-09 06:33
User-Agent: Microsoft Outlook Express 6.00.2600.0000



Dear Customer,

As the Internet and information technology enable us to expand our services, we are committed to maintaining the trust customers have placed in us for protecting the privacy and security of information we have about you. In order to protect your information against unauthorized access, identity theft and account fraud we earnestly ask you to update your profile.

Check security.calpoly.edu...

http://security.calpoly.edu/what_everyone/spam_alert.html

The screenshot shows a Mozilla Firefox browser window with the address bar containing http://security.calpoly.edu/what_everyone/spam_alert.html. The page header features the Cal Poly logo and the text "Information Security" and "California Polytechnic State University". The main content area is titled "SPAM Alerts" and contains several sections of text:

- SPAM Alerts**: Below are examples of recent SPAM received by abuse@calpoly.edu. Most messages are being tagged as cpSPAM so recipients can easily filter and delete them. However, messages appearing to come from a campus email address are not tagged by Cal Poly's anti-spam gateway and will continue to be delivered. For more information on how to identify, filter and deal with SPAM, please visit: <http://www.email.calpoly.edu/spam/>
- INVESTMENT "TIPS" WITH UNRELATED SUBJECT LINE (12/21/06)**: A new variation of the investment tip SPAM (junk e-mail) is now circulating on campus. The subject line has no relationship to the message content and there is no graphic included. The subject line often matches the first name of the purported sender, e.g., ("John" from "John Doe"). The message generally begins with a single line ("The hottest pick this year!" or "This could be your big break!") and goes on to promote a specific stock. The stock being promoted may vary from week-to-week.
- DISCOUNT SOFTWARE-RELATED MESSAGES (12/18/06)**: Two varieties of SPAM messages promoting sales of software are being received by Cal Poly users. The first may open with the line "Dear customers and friends of DS Team". It describes a special offer to sell the recipient a Windows Vista Ultimate Upgrade at a reduced rate. The second sometimes contains the subject line "Buy OEM Software" and begins with the single line "Top 10 Items Now" or "All Titles on Sale". Both variations offer special discounts on Windows, Adobe and other software products.
- PHRASE IN SUBJECT LINE, IMAGE FILES, RANDOM TEXT (Updated 12/21/06)**: Campus users continue to receive messages with odd subject lines but instead of a few words, the latest variation uses a random phrase or sentence as the subject line. Each message includes at least one small graphic file (.gif) as an attachment, and a text message consisting of a single word in the first line followed by a series of often unrelated sentences. The graphic contains a multi-colored background with a text message promoting a penny stock, replica watches or other items for sale. In a new variation, the message text is capitalized and contains weather-related information.

The left sidebar contains a navigation menu with links such as "Information Security: Top Ten", "What Employees Should Know", "What Everyone Should Know", "What Technical Support Staff Should Know", "Policies", "Report a Violation", and "Contact Us". There is also a search box for "Information Security".

The standard stuff...

- Campus provides:
 - Anti-spyware
 - Anti-virus
 - Windows updates process
- Use them!

Ask “Why do you need that?”

- When asked for information, you have a choice ...
(what’s in it for _____)

Detect – Check your credit report

- Visit

<http://www.AnnualCreditReport.com>

- Free, once a year

- Report unexpected accounts immediately

Take Inventory

- What's in *your* wallet?
- <http://www.idtheftcenter.org/>
 - Social Security number (SSN) usually printed on card
 - Driver's license - Did it have your SSN on it? Yes No
 - Credit cards (itemize)
 - Vehicle registration papers
 - ATM/ Debit cards/ Bank cards
 - Check cashing card, bank checks (your own account)
 - Your Social Security card **

Act....

- If you believe personally identifying information has been lost or stolen:
 - request a “fraud alert” be placed
 - see <http://www.ftc.gov> for details

Remember...

- Identity = information = *money*
- You'll do (so take precautions)
- Be vigilant
- Report suspicious activity

Further information...

- Federal Trade Commission Identity Theft site: <http://www.ftc.gov/idtheft/>
- Cal Poly Security site: <http://security.calpoly.edu/>

QUESTIONS?

security@calpoly.edu

Vicki Stover

SSN: 078-05-1120

Ryan Matteson

SSN: 078-05-021