Security

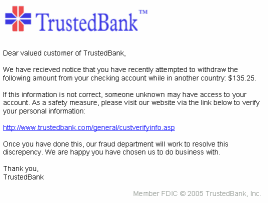
Chapter 12

What Should I Ask Santa Claus For?

- **e-mail spoofing**: fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source

Phishing

- **phishing**: scam by which an e-mail user is duped into revealing sensitive information such as passwords and credit card details


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Link might go to another website (links are easy to spoof); hover mouse over links to see where they lead

What Can Be Done About Phishing?

- Never respond to requests for personal information like passwords via e-mail (or phone!).
  - Legitimate businesses do not request such information this way.
- Visit web sites of companies with which you have business by manually typing the company URL.
  - Do not click on links in unexpected e-mails because they can be spoofed.
  - Along the same lines, do not call phone numbers found in those e-mails.

What Can Be Done About Phishing?

- Be leery of URLs that do not have the company name directly before the top-level domain.
  - For example, bankofamerica.com is the correct URL, bankofamerica.pp.com is questionable.
- Routinely review your credit card and bank statements for unusual activity.
  - http://annualcreditreport.com
- "Recognizing Phishing Scams and Fraudulent / Hoax Email"
  - http://www.microsoft.com/protect/yourself/phishing/identify.mspx

How Often Should You Change Your Passwords?

- https://uwnetid.washington.edu/manage/
- Can't an attacker (perhaps using a computer program) keep guessing passwords?
  - Computer systems usually impose a time-out of several seconds after a number (e.g. three) failed attempts.
- "Top 10 Most Common Passwords"
  - http://modernl.com/article/top-10-most-common-passwords

Social Engineering

- **social engineering**: the act of manipulating people into performing actions or divulging confidential information

7

Password Insecurity

- Source: "Palin E-Mail Hacker Says It Was Easy"
  - http://blog.wired.com/27bstroke6/2008/09/palin-e-mail-ha.html
- "As detailed in the postings, the Palin hack didn't require any real skill. Instead, the hacker simply reset Palin's password using her birthdate, ZIP code and information about where she met her spouse -- the security question on her Yahoo account, which was answered (Wasilla High) by a simple Google search."

8

Malware

- **malware** (**mal**icious soft**ware**): software designed to infiltrate or damage a computer system without the owner's informed consent
- **computer virus**: catch-all phrase to include all types of malware, including true viruses
- Other terms for baddies: trojan horse, worm, adware, spyware

9

How Malware Spreads

- Some malware can be secretly installed just by visiting infected web sites.
- Others require human intervention to propagate (e.g. clicking on an e-mail attachment or installing infected software)

10

How Malware Spreads

- USB drives can be carriers of computer viruses.
- Window that pops up when you insert an infected USB drive looks similar to that when inserting a clean USB drive.
  - Clicking icon infects the computer.
  - To prevent further infection, click the X on the top right.
  - However clean drives can still be infected just by using the USB drive with an infected computer.

11

What's The Worst That Could Happen?

- **keylogger**: software that can capture and record user keystrokes
- **backdoor**: hidden method for bypassing normal computer authentication systems
- **zombie**: computer attached to the Internet that has been compromised
- **denial-of-service attack** (**DoS attack**): attempt to make a computer resource unavailable

12

Preventative Tips

- Show hidden files. If you do not know what a file is for, look it up on the web.
  - http://www.microsoft.com/windowsxp/using/helpandsupport/learnmore/tips/hiddenfiles.mspx
- Do not open unexpected e-mail attachments.
- Be wary of pop-up windows that ask you to install something (like anti-virus software) if you are just surfing the web.

13

Preventative Tips

- Keep your system up-to-date. Newer systems automatically update.
  - Verify that your computer automatically updates or make sure to manually update every so often.
    - http://windowsupdate.microsoft.com
  - If you must use IE, use the latest version.

14

Useful Software: Firewall

- **firewall**: software which inspects network traffic passing through it, and denies or permits passage based on a set of rules
  - Most systems have firewalls installed.

15

Useful Software

- "Protecting your computer from viruses"
  - http://www.washington.edu/computing/virus.html
  - Contains link to anti-virus software for both Mac and Windows
- Additional Windows Software
  - Ad-Aware
  - Spybot – Search & Destroy
  - AVG Anti-Virus

16

An Ongoing Battle…

ALERT - VIRUS INFECTS SOME UW STUDENT COMPUTING FACILITIES
Date: 03/06/2009

Today, the Conficker worm infected a number of older machines in several student computing facilities on campus. It is a common virus that has exploited and infected millions of Windows operating systems across the globe.

Currently, we are working hard to repair the infected machines. We expect network connectivity to be restored to these machine later today.

We would like to share our commitment to the University of Washington students to maintain a 95% functionality rate for the sit-down workstations in the Odegaard Library and the Mary Gates Hall Technology Spaces and a 90% functionality rate for the stand-up computing workstations in the various campus libraries.

If your personal computer becomes infected with the Conficker worm, you can visit the McAfee website for tips on how to remove it. Or, take advantage of the Computer Vet– a free, help-desk service offered to UW students, faculty and staff to assist with computing problems including virus infected computers blocked from UW network access. Computer Vet is available at the Technology Help Desks in Computing Commons in Odegaard Undergraduate Library and Mary Gates Hall. You can also prevent your personal computer from becoming infected by running all Windows updates, or visiting this MS knowledge base article to directly download the patch.

The student computers in Odegaard Library are funded by the Student Technology Fee, not through tuition or state funds.

17

Cleaning Viruses

- Anti-virus software is only good if you keep it up-to-date.
  - New viruses are coming out all the time.
- In certain cases, you may have to clean a virus manually.
  - Try to find respectable directions on the web. The process can be very tedious.
- Computer Vet
  - http://www.washington.edu/computing/computervet/

18

For Your Security

- Don't save important passwords in your browser.
  - What if someone steals your computer?

Secure Protocols

- **Hypertext Transfer Protocol Secure** (**HTTPS**): combination of HTTP and a network security protocol
  - URL begins with https://

notice the 's'

lock indicates secure website

Spam!

- **spam**: unsolicited or undesired electronic messages
  - Usually sent by zombie computers.

Is Anyone Dumb Enough To Respond To Spam?

- One study showed that the hit rate for pharmaceutical spam is about 1 in 12 million.
- Source: "Spamalytics: An Empirical Analysis of Spam Marketing Conversion"
  - http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf
  - Spam Targets: 347,590,389
  - User Conversions: 28 (0.0000081%)

Preventing Spam

- **CAPTCHA**: **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

E-mail

- Some e-mail programs do not show certain images in the e-mail unless you press another button. Why?
  - This concern images that have to be downloaded from another source (vs. just being attached to the e-mail).
  - Fetching images can alert the sender that the e-mail address is valid. So what?
    - Spammers love valid e-mail addresses!