
I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFOR-MATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.
www.dilbert.com scottadams@aol.com
8-12-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.

Information Security Open Forum

- Information security updates
- Epsilon Breach - what you should know
- How to stay safe while “browsing the Internet”

Wednesday, April 27, 2011
University Union 220

Terry Vahey, Chris Call,
Mike Cook, Tim Schmidt

Information Security Updates

- Due May 2011
  - Risk Self-Assessments
  - Confidential Level 1 on workstations
  - Retention & Disposition Schedules
- Confidential shred info:
  - http://www.afd.calpoly.edu/facilities/sitemap.asp
  - Also listed under recycling

Epsilon Breach Concerns

- Spam (annoying - usually unrealistic)
  - Unsolicited bulk messages
  - Lottery winner
- Phishing email (scary)
  - Attempts to get your personal information using generic data
  - “Sender” may not be familiar
- Spear-phishing email (very scary)
  - Attempts to get your personal information using actual facts in a targeted message
  - Always a “sender” you’ve done business with

Example of a Phishing Email

----- Forwarded Message -----
From: “CITIBANK SUPPORT"
Subject: Account Upgrade

Dear Valued Member,

To update your account and insure that your frequent flyer miles carry over, you are required to reply to this mail with your username and password in the spaces provided below or your account will be terminated within the next 48hours and your frequent flyer miles will be void.

Username:
Password:

CITIBANK ACCOUNT TECHNICAL SUPPORT

Example of a Spear-Phishing Email

----- Forwarded Message -----
From: “CITIBANK SUPPORT"
Subject: Account Security Upgrade

Dear Chris Call,

To update your account and transfer your 75,340 frequent flyer miles, reply to upgradeaccount@Citibank1134mike.com You are required to change your password and will be asked to provide your old username and password to receive a new password prompt.

Your account will be terminated within the next 48hours and your frequent flyer miles will be void if we don’t hear from you.

CITIBANK SECURITY TEAM

Scam Alert

- Reputable companies do not email requests for:
  - Login credentials
  - Credit card numbers
  - Bank account info
  - Social security cards
- If in doubt:
  - Contact the source using information **you** have
  - Do not use link provided within email message
- Examples

Examples - Phishing Site

- Bad guys create fake web pages
  - No special applications
  - Create site using real logo - less than 4 minutes
  - Create fake payment site - 3 minutes
- Bad guys create phishing email messages
  - No special application
  - Create message using a real logo - 5 minutes
- Total time to steal information
  - Less than 15 minutes

Phishing Challenge

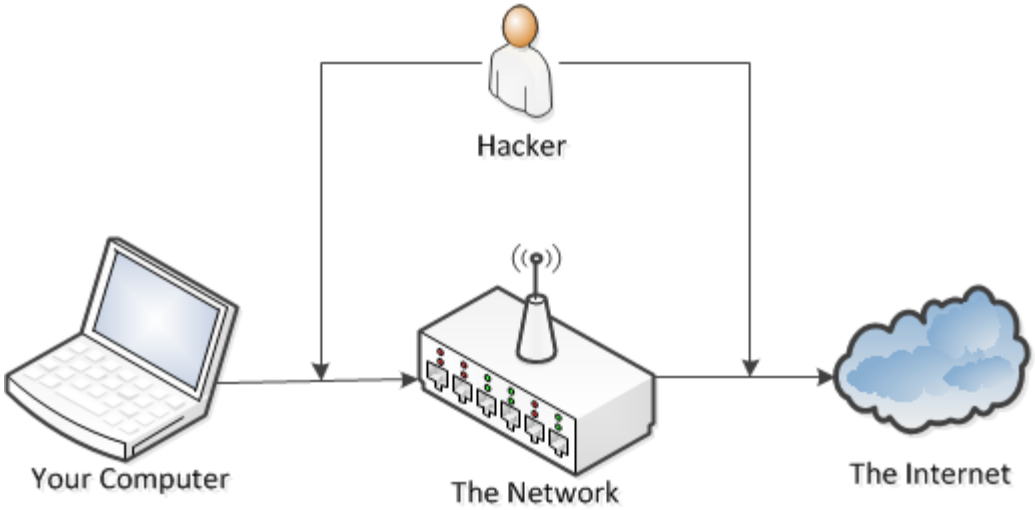
- Take the phishing challenge
  - https://www.phish-no-phish.com/default.aspx

Safe Internet Browsing

- Trust the computing device
  - Is it secure?
- Trust where you are going
  - Is it secure?
- Trust the network
  - Is it secure?

Where Can Someone Gain Access to Your Data?

- An unsecure computer
- An unsecure Web site
- An unsecure network



Is My Computer Secure?

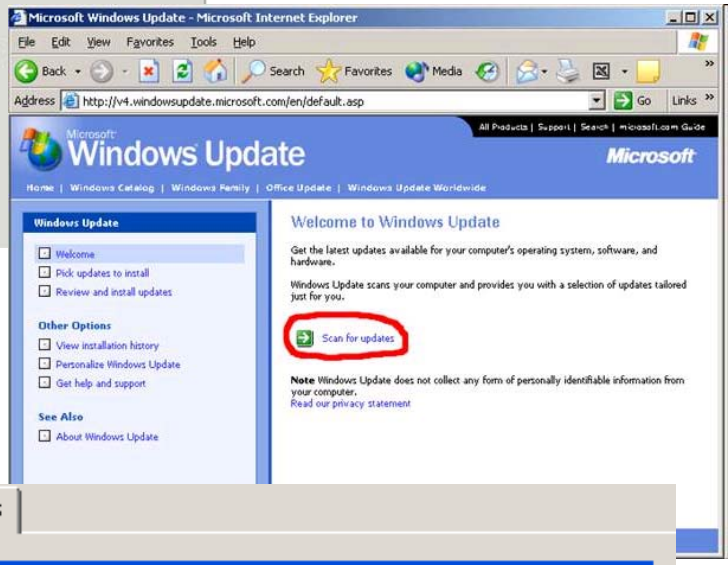
Trust the computing device

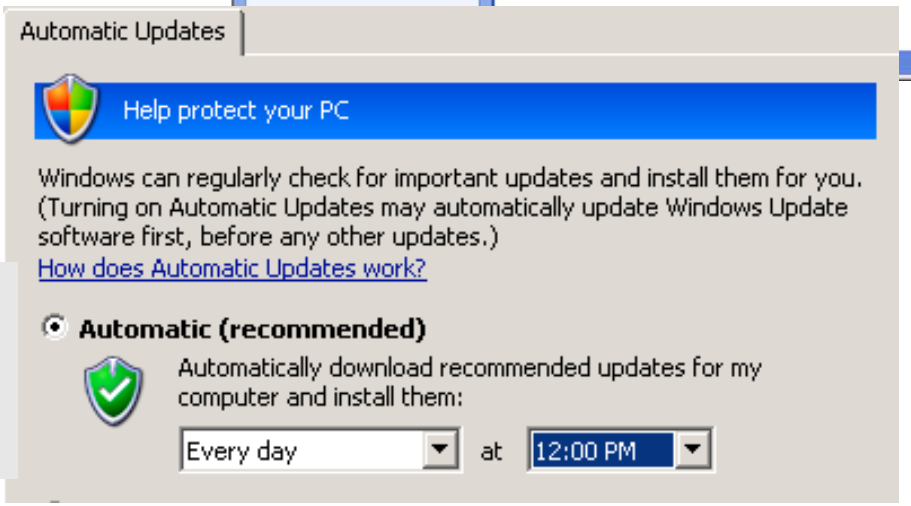
- Use trusted applications
  - Keep your software updated
- Use anti-virus and firewall software
- Be wary of suspicious emails, updates, pop-ups, and links
  - If in doubt, get out!
- Use strong passwords

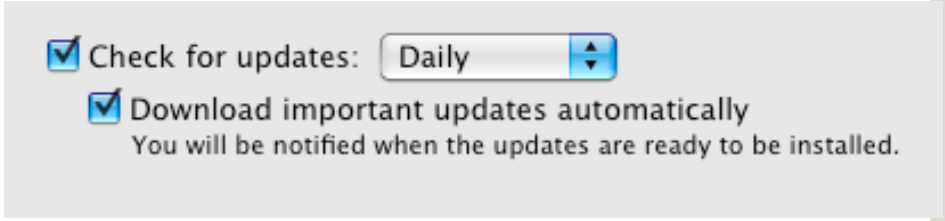
Keep Software Updated

Regularly update your computer software

- Operating system
- Browser
- Other Applications

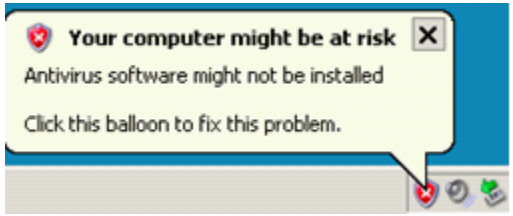


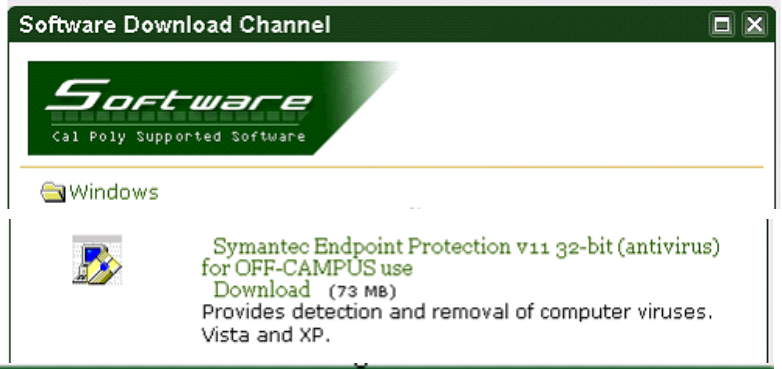


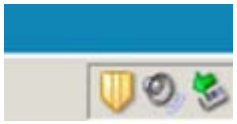


Use Anti-Virus

- Download it for free at my.calpoly.edu
  (Free to Cal Poly faculty, staff, students)
- Keep definitions updated- Set to automatic updates

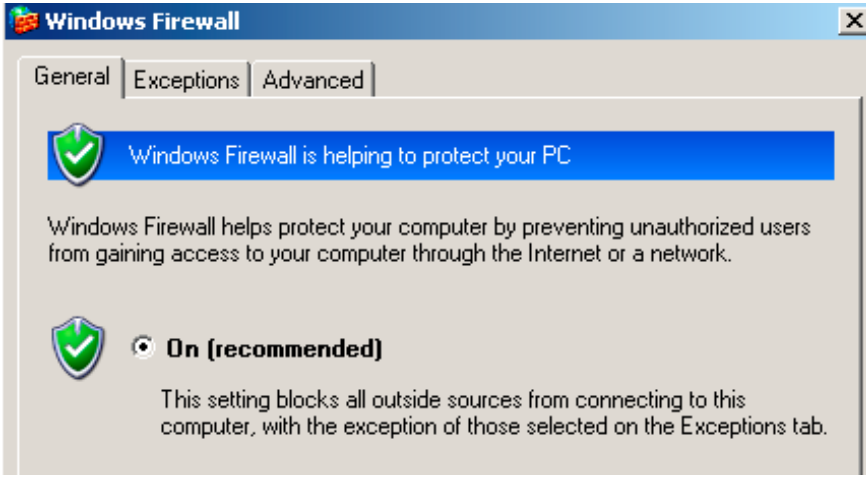


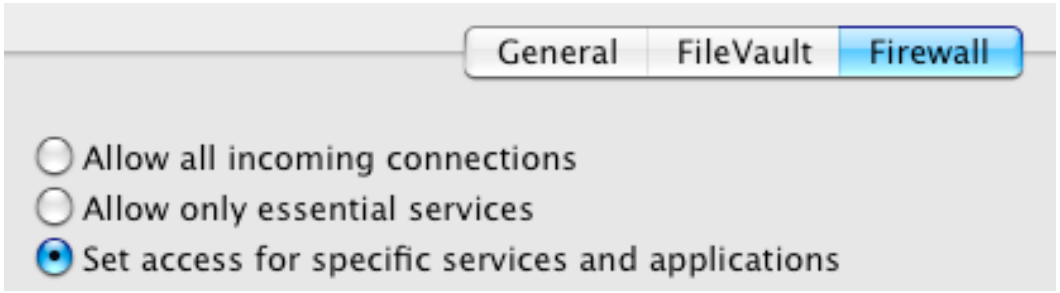




Enable Firewalls

- Use operating system firewall
- For personal computers
  - Buy an Internet Security Suite

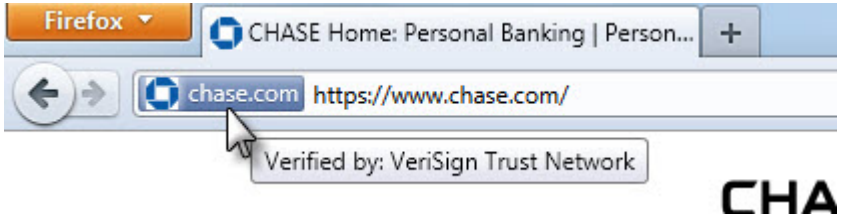


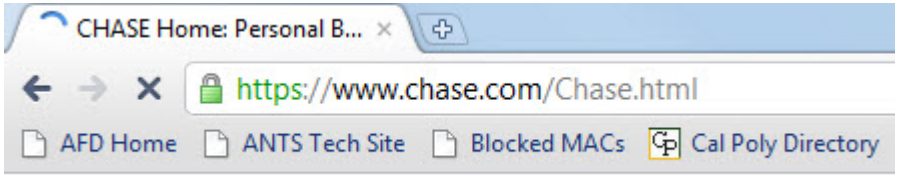


Is The Web Site Secure?

Trust where you are going

- Is it an HTTPS site?
- Is the site reputable?
- Do I feel safe using the site?
  - Use the Gut-Feeling test
  - Sample Suspect Site
  - Sample Good Site



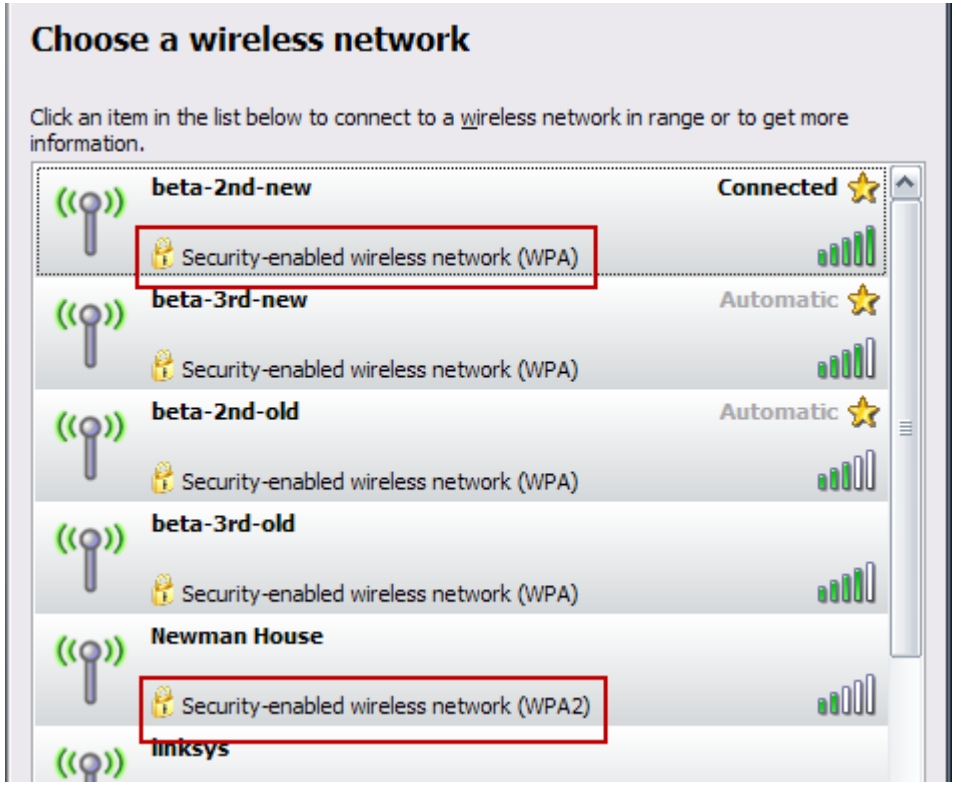


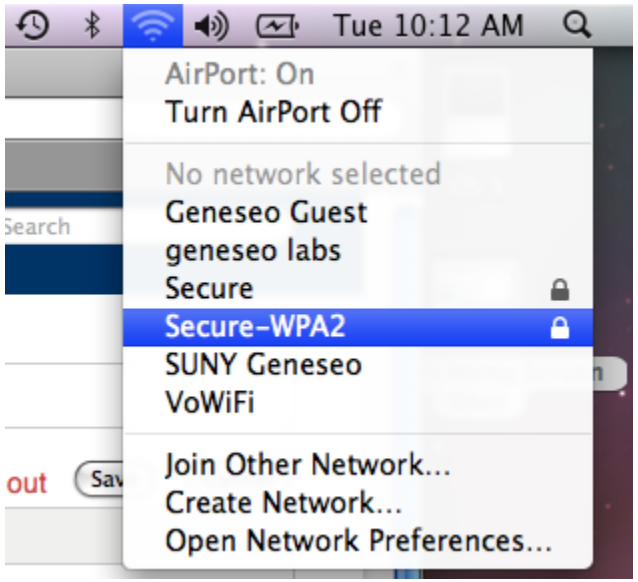
Is My Network Secure?

Trust the network

- Home
  - Use encrypted wireless (WPA2 preferred)
    - Information Security Open Forum Presentation- October 2010
- Work
  - Verify with your LAN Coordinator
- In Public
  - Is it encrypted (WPA2 preferred)?
  - Who has access to the network?
    - Do I trust the people connected to the network?

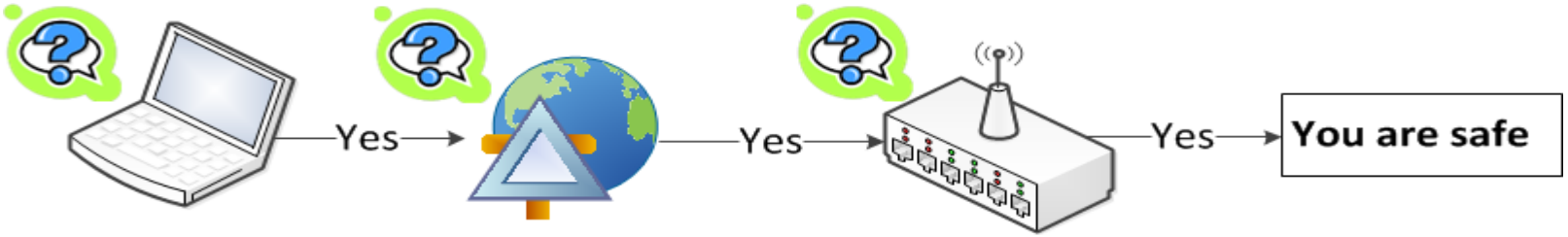
Is My Network Secure?





Scenario #1

- I trust my computer
  - Updated software, Antivirus, Firewall
- I trust the site I am accessing
  - https://
- I trust my network
  - secured with WPA2
- Does this mean I am safe browsing anywhere?
  - Yes



Scenario #2

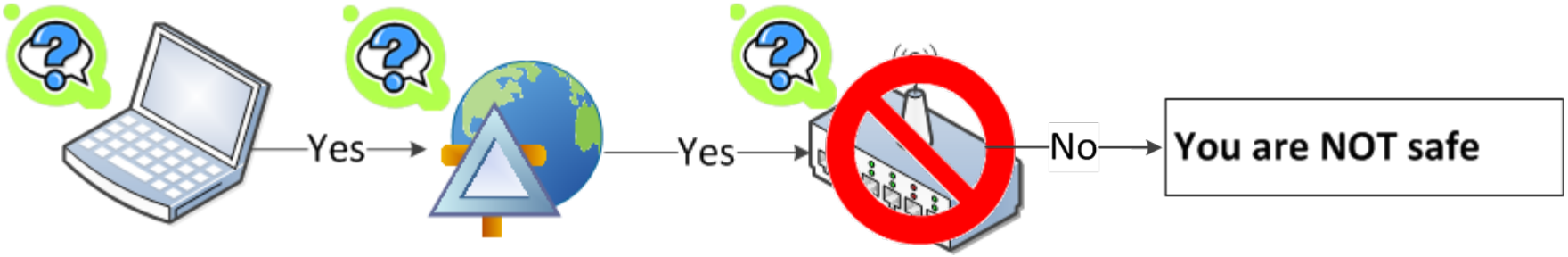
- I do not trust my computer
  - I'm using the hotel lobby computer
- I trust the site I am accessing is secured
  - https://
- I do not trust my network & those on it
  - It has already connected to the Internet for me!
- Does this mean I am safe browsing anywhere?
  - No

No

Stop! You are NOT safe. Do not provide personal information

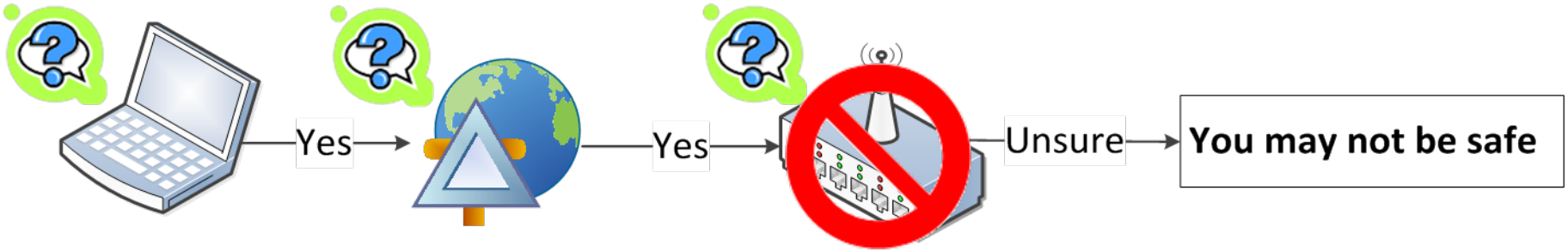
Scenario #3

- I trust my computer
  - Updated software, Antivirus, Firewall
- I trust the site I am accessing
  - https://
- I do not trust my network & those using it
  - The hotel gave me this convenient & obvious password
  - Starbucks is concerned about my computer, right? <not>
- Does this mean I am safe browsing?
  - Consider this “No”



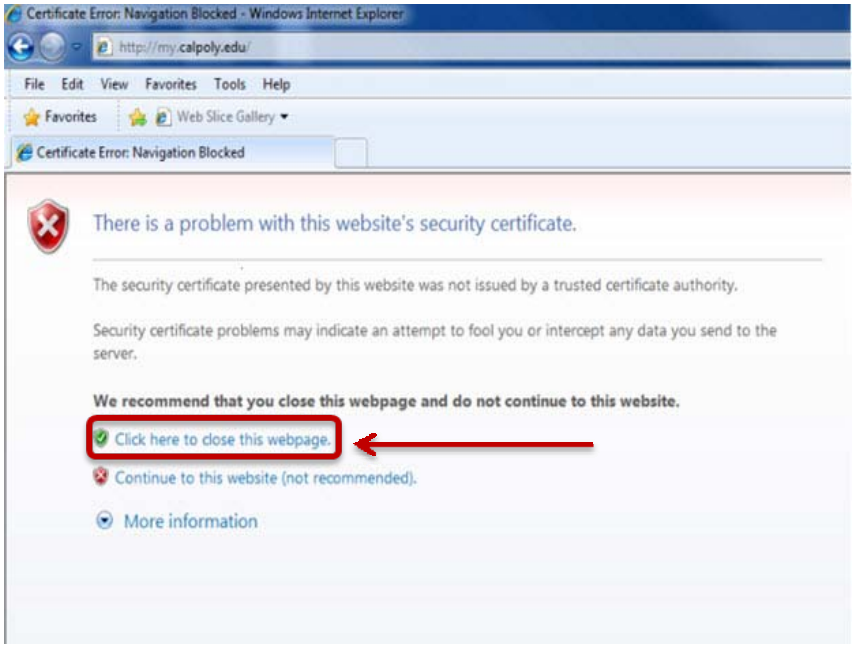
Scenario #4

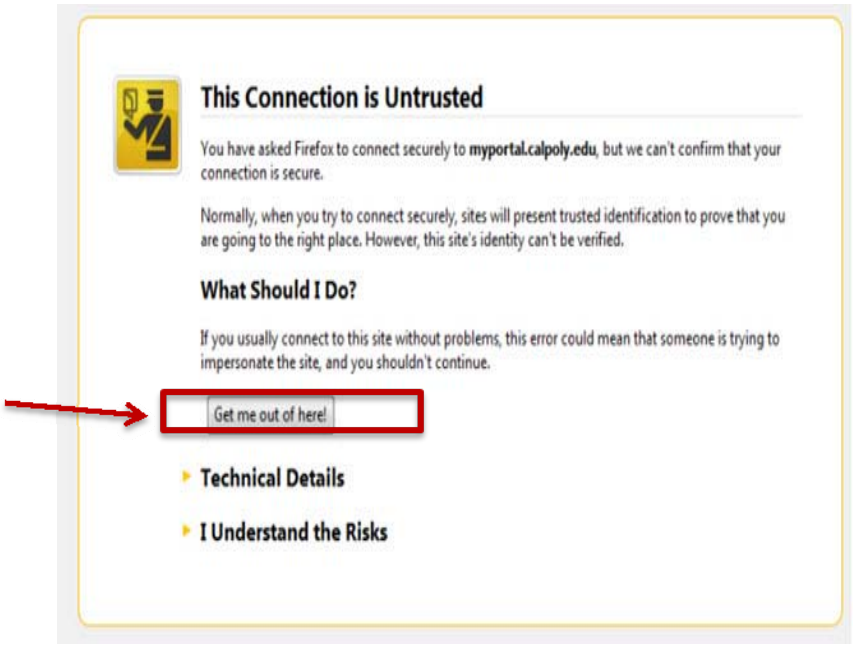
- I trust my computer
  - Updated software, Antivirus, Firewall
- I trust the site I am accessing
  - https://
- I'm not sure about the network
- Does this mean I am safe browsing? **You may not be safe**
  - Avoid entering confidential information until you have a more secure network connection.
  - Read, understand, and heed ALL browser warnings you see (i.e. pop-ups.)
  - Beware of unusual computer behavior- operating extremely slowly (indication of snooping).
  - Consider alternative connections such as a cell phone.



Read and Understand Warnings

- Certificate Warnings
- Someone could be snooping your info!





Read and Understand Warnings

- Mixed Mode Warnings and other popups?

Safe Computing Guide

Question #1

Do I trust the computer I am using?

- Patched/Updated
- Anti-Virus
- Firewall

Yes

Question #2

Do I trust the site I am accessing?

- Is it reputable?
- HTTPS
- Is it certified?

Yes

Question #3

Do I trust the network?

- Encrypted (WPA2)
- Is access resticted to the public?
- Who else is on the network?

Yes

You are safe to browse the Internet

Unsure

You may not be safe

Follow these guidelines to reduce your risk

- Avoid entering confidential information until you have a more secure network connection.
- Read, understand, and heed ALL browser warnings you see (i.e. pop-ups.)
- Beware of unusual computer behavior- operating extremely slowly (indication of snooping).
- Consider alternative connections such as a cell phone.

No

No

No

You are not safe

You could lose:

My money in the bank
Access to change student grades
Access to purchase with P-card
Access to PeopleSoft

SSN #'s including your own
Cal Poly's reputation and your own
Your bank accounts and credit cards
Your identity

Don’t put your head in the sand!

Identity Theft Stats - 2010

- Florida highest per capita rate of reporting
  - Arizona
  - California
- Data breaches are a big deal!
  - 8x more likely to be a victim if you receive notice
- Cost- out of pocket expense
  - $387 per incident (2009)
  - $631 per incident (2010)

Source:
http://www.washingtonpost.com/wpdyn/content/article/2011/02/09/AR2011020906064.html

Remember - Protect Yourself

- Protect your computer
- Use secure Internet connections
- Don’t click on embedded links in email
- Monitor your bank accounts – more than 1x month
- Use strong passwords
- **Always assume you could be at risk**

Pay Attention & Be Alert

Questions?

Thank you for your participation!

Today's slide presentation, Cal Poly policies and standards, how-to's, along with additional materials are posted at http://security.calpoly.edu

Terry Vahey, tvahey@calpoly.edu, 756-7667
Chris Call, ccall@calpoly.edu, 756-7622
Mike Cook, macook@calpoly.edu, 756-7372
Tim Schmidt, tschmidt@calpoly.edu, 756-2848