

Internet Safety



Detective John Alvarez
High Technology Crimes Unit
Corona Police Department



Topics Covered

- Malware (Viruses, Spyware & Adware)
- Internet Safety
- Website Security
- Alternate Web Browsers
- Alternate Operating Systems
- Firewalls
- Wireless Networks
- “Phishing” Scams
- Sexual Predators



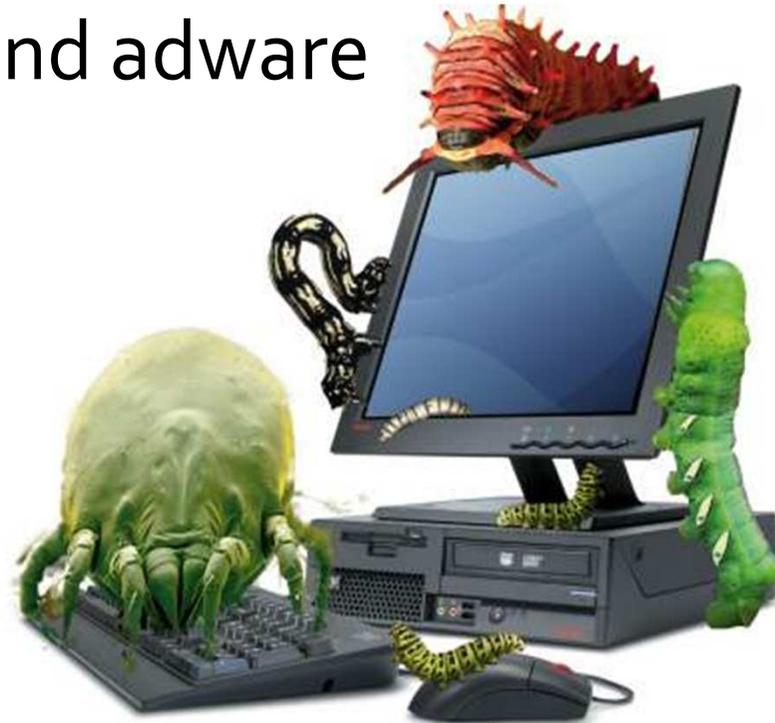
Disclaimer

- This can be an in-depth subject, but this document is just an overview.
- I recommend products I have tested and prefer, but there may be plenty of other fine products available.
- I have no vested interest in any of the recommended products.
- Online threats change by the minute so something I discuss may change by the time you go online.

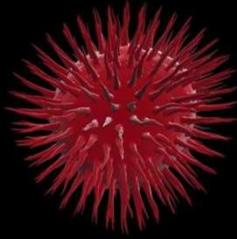


Malware

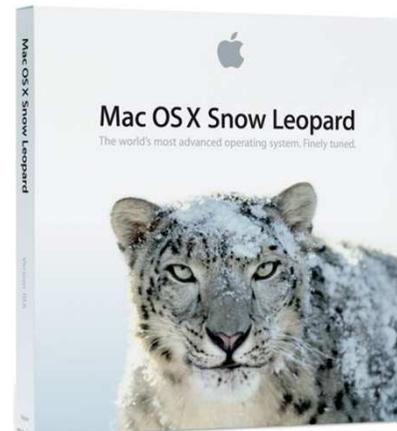
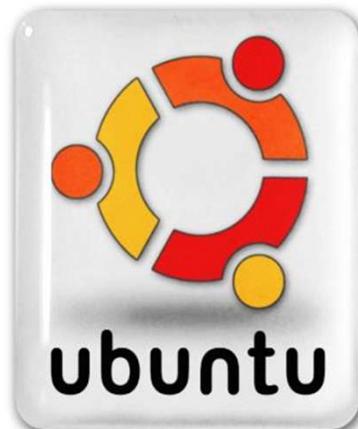
- The term “malware” includes viruses, spyware and adware



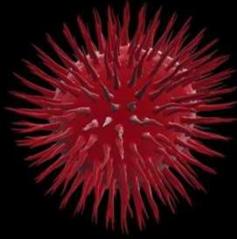
Viruses



- Most malware programs are written to infect computers running the Microsoft Windows operating system. Apple and Linux operating systems are not completely safe from malware, *but the risks are significantly less.*

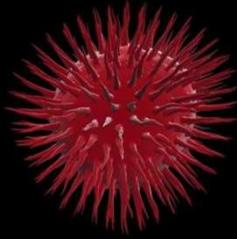


Viruses



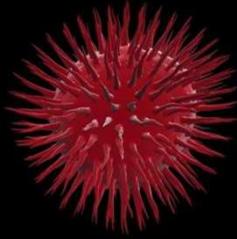
- A computer virus is a program that can copy itself and infect a computer without permission or knowledge of the user.
- Some viruses are programmed to damage programs, delete files, or reformat the hard disk.

Viruses



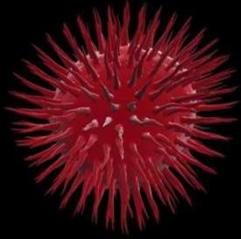
- Some viruses steal your personal information, such as credit card numbers, bank account information, usernames, passwords, etc. These viruses send the gathered information to waiting criminals.

Viruses



- Some get between you and your bank and change the destination of transfers. These are known as “man-in-the-middle” viruses.
- Some viruses spread to as many computers as possible to mount an attack against a particular website (known as a **Denial Of Service** attack).

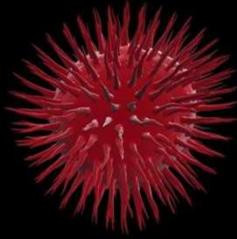
Viruses



- Is your computer a zombie?



Viruses



- Your computer is a “zombie” when it is taken over and used for illicit purposes (spamming, pirated software, child pornography, etc.).
- Why would a criminal want to risk using their own computer when they can use yours?
- It may be quite a while before you even know this is going on.

Spyware



- Spyware is computer software that is installed surreptitiously on a computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.
- Spyware is also known as **malware**.
- Spyware is very similar to a virus and many times is detected by virus scanners.

Spyware



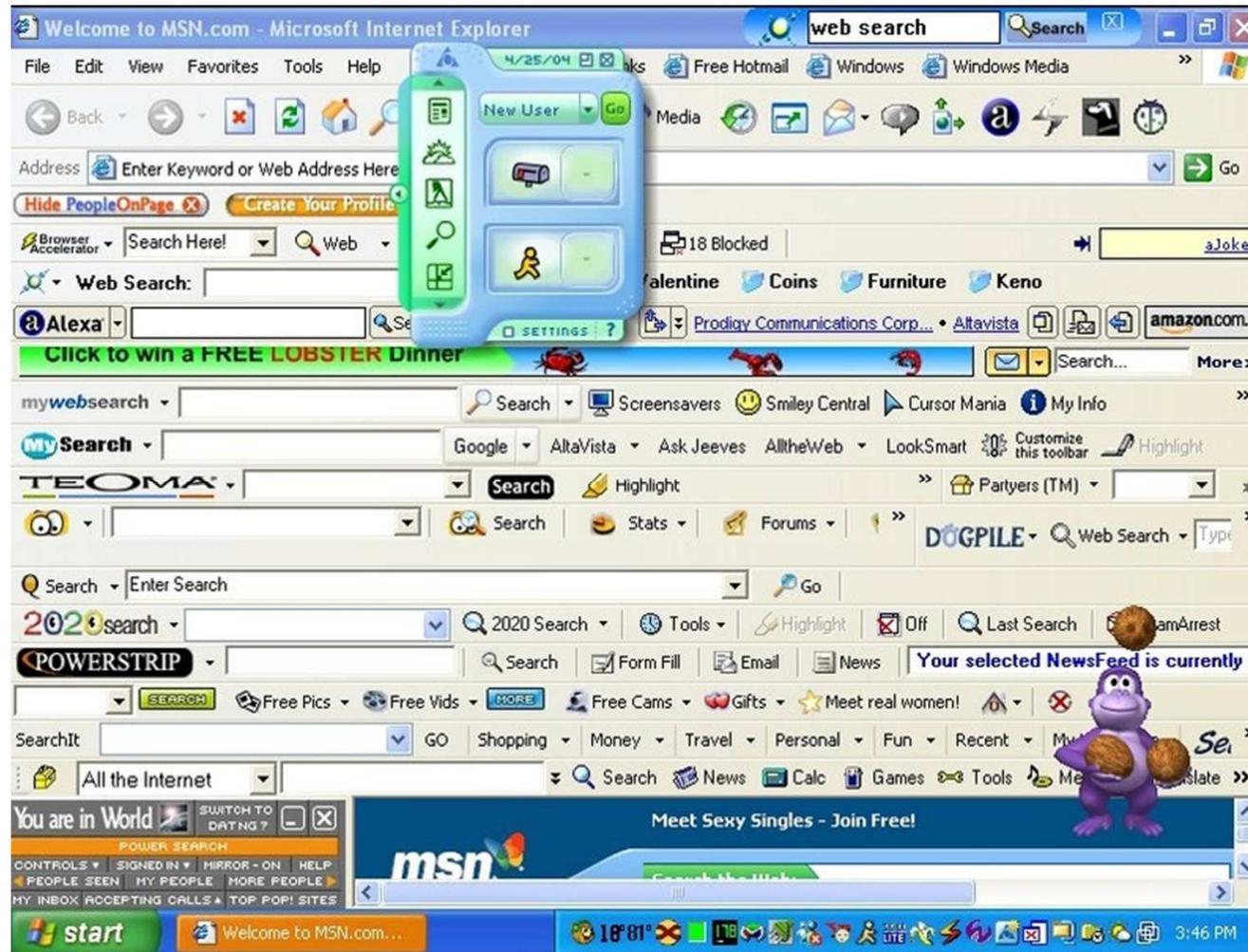
- While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring.
- Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party.

Spyware



- Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.
- If your web browser looks like this, you have a spyware problem...

Spyware



Adware

FREE MONEY!
Sign up a friend to AOL and get **\$25!**
Click Here for Details!



CONGRATULATIONS!

You've been chosen to receive a **FREE Gateway Desktop Computer!**

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (19-inch viewable)

FREE!

Click Here to Claim Your **FREE** Desktop Computer!

POKER ON-NET

Download Getting Started Features Contact Us Help

Current Events

Double \$5,000

Blackjack Roulette Slot Machine **Click Here!**

Click OK to download our free software while browsing the site.

Start | SLOON.COM - Fed... | WELCOME TO CASINO... | Online Poker Room: T... | http://ad1.revolve... | 6:09 PM

Adware



- Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.
- Adware is not much of a problem these days.



How Does Malware Spread?

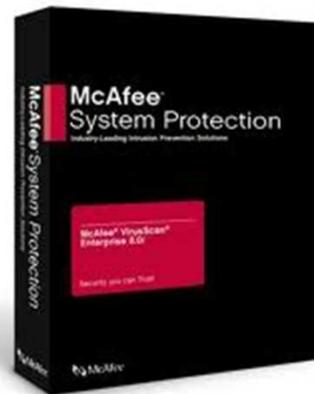
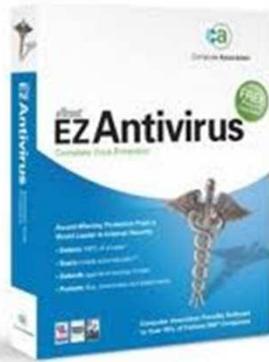
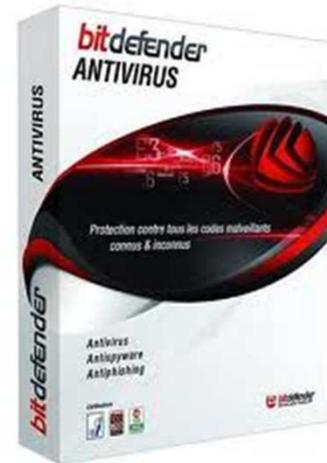
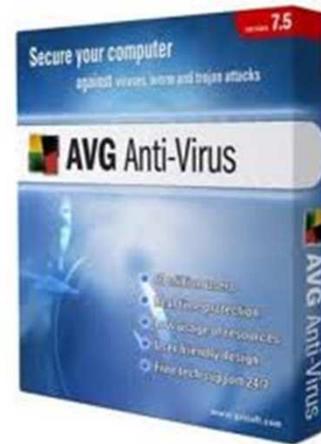
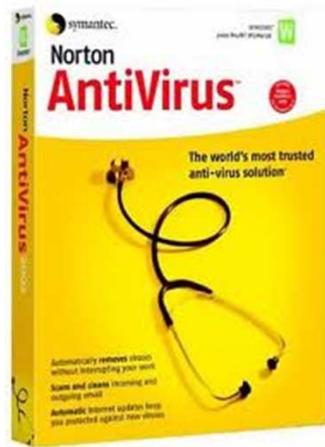
- You may install a program that is infected with malware or is not even the program you think it is.
- You open an infected email attachment.
- Malware can access your email contacts then email itself to everyone you know!
- You visit a website engineered to install malware via web browser vulnerabilities.



How Does Malware Spread?

- No antivirus and/or spyware programs installed.
- Antivirus/spyware scanners not up-to-date.
- Insufficient antivirus and spyware scanners (some antivirus scanners are shut down by some viruses).
- No firewall. The W32.Sasser.Worm scans the internet for unprotected computers. This virus can spread without the help of the user.

Virus Scanners



Virus Scanners



- Use effective antivirus and spyware scanners.
- *It does not mean a virus scanner is effective just because it comes installed on most new computers. That is just good marketing.
- Choose a virus scanner based on your threat level and reviews by trusted sources (PC Magazine, PC World, etc.).
- Avoid buying solely on the recommendation of sales personnel in big chain electronics stores. They will sell you what they have to offer and what makes them money. Many of the better virus scanners are not sold at big chain stores.

Virus Scanners



- An effective virus scanner is updated often. Virus scanners need to be able to recognize new threats as soon as possible.
- Scan your system often (weekly or daily).
- Besides a virus scanner, you also need to run anti-spyware/adware programs. The list of these products can be overwhelming. You can start with free and trustworthy programs like Malwarebytes' Anti-Malware.



Change Your Online Habits

- Human behavior helps spread malware. Few malware programs are installed without some type of human interaction.
- Avoid websites that deal with illicit or adult content (pornography, gambling, “warez,” etc.).
- Avoid file sharing programs. These programs can be used for legitimate purposes, but most often are used for illegal activity - a perfect environment for the spread of malware.





Change Your Online Habits

- If something unsolicited pops up on your screen – **DO NOT DOWNLOAD IT!** Unsolicited programs are many times malware.
- A popup message might even say your system is infected with spyware and the program being advertised will help remove it – **DO NOT BELIEVE IT!**
- Do not open email attachments from people you do not know.



Change Your Online Habits

- Be careful opening email attachments from people you do know. Remember, a virus might be sending you an email from your friend's computer without their knowledge.
- If an email from a friend comes with an attachment not consistent with something they would normally send – **DO NOT OPEN IT!**



Change Your Online Habits

- An email saying it is from a friend can be “spoofed” (faked). It may not really be from them so be suspicious of emails that seem out of character.
- Do not respond to spam emails because this will only confirm your email address is valid.
- Do not click on links in spam emails. Some may send you to a website that can infect your computer merely by visiting.



Extra Suggestions

- Monitor teenagers! Teenagers will download and install almost anything!
- Keep your operating system and programs updated. You can have your system infected by malware simply by not having all updates installed.

Social Networks



- Be careful what you post online!
- Some people put enough information on these sites to be used by criminals.
- Social networks are not very secure or blatantly expose and/or sell your information.
- If you work in a career where posting your photos and information can put you and your family at risk – don't do it!

Social Networks



- The person in charge of MI6 may have some enemies...

MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving

By JASON LEWIS
Last updated at 7:14 PM on 5th July 2009

[Comments \(104\)](#) [Add to My Stories](#)

The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain's spying operations abroad.

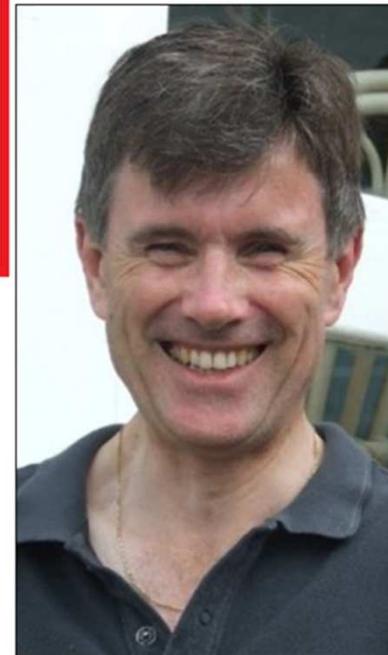
But his wife's entries on the social networking site have exposed potentially compromising details about where they live and work, who their friends are and where they spend their holidays.

Amazingly, she had put virtually no privacy protection on her account, making it visible to any of the site's 200million users who chose to be in the open-access 'London' network - regardless of where in the world they actually were.

There are fears that the hugely embarrassing blunder may have compromised the safety of Sir John's family and friends.

Lady Shelley Sawers' extraordinary lapse exposed the couple's friendships with senior diplomats and well-known actors, including Moir Leslie, who plays a leading character in *The Archers*. And it revealed that the intelligence chief's brother-in-law - who holidayed with him last month - is an associate of the controversial Right-wing historian David Irving.

Immediately after *The Mail* on Sunday alerted



Website Security



- Is a website secure? Is it even legitimate?
- When dealing with any website that will involve the exchange of sensitive information, make sure the information is secure/encrypted.
- How do you know when a website is secure/encrypted? Look for the “S” and the padlock. Secure websites will begin with **HTTPS**.

Website Security

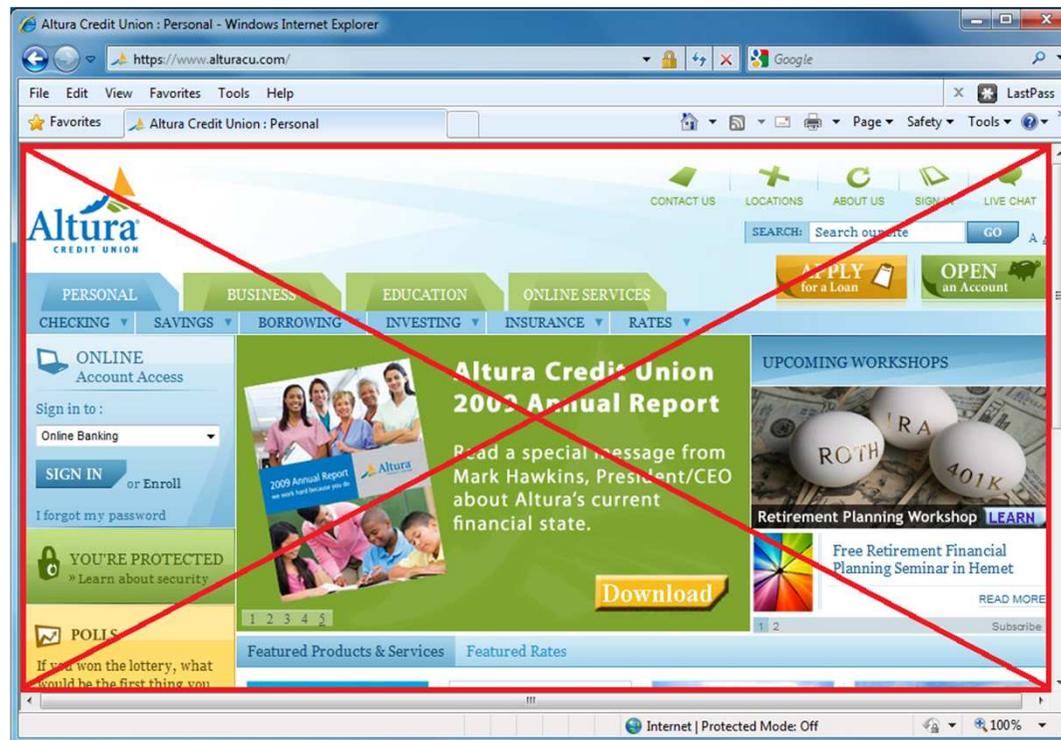


- Security/encryption may only take place when it comes to a web page where the actual exchange of information will take place.
- Example: You go to the main page of your banking website and there is no encryption:
<http://www.yourbank.com>
- You select the online banking link and then you are sent to an encrypted web page where the exchange of sensitive information takes place:
<https://www.yourbank.com>

Legitimate Padlock Location



- A padlock icon may be present on a secure website and should be in the frame of the web browser.
- The padlock should not be on the web page itself.



Website Security



Altura Credit Union : Personal - Windows Internet Explorer

https://www.alturacu.com/

Altura CREDIT UNION

PERSONAL BUSINESS EDUCATION ONLINE SERVICES

CHECKING SAVINGS BORROWING INVESTING INSURANCE RATES

ONLINE Account Access

Sign in to:
Online Banking

SIGN IN or Enroll

I forgot my password

YOU'RE PROTECTED
» Learn about security

POLLS
If you won the lottery, what would be the first thing you

Altura Credit Union 2009 Annual Report

Read a special message from Mark Hawkins, President/CEO about Altura's current financial state.

Download

UPCOMING WORKSHOPS

Retirement Planning Workshop LEARN

Free Retirement Financial Planning Seminar in Hemet

READ MORE

Internet | Protected Mode: Off

Website Security



A screenshot of a web browser window. The address bar shows the URL "https://www.alturacu.com/personal" with a green padlock icon to its left, which is highlighted by a red rectangular box. The browser's toolbar includes back, forward, and refresh buttons, along with various extension icons. Below the address bar, there are several bookmarks for Gmail, Google Reader, Google Voice, Windows Live Hotm..., and Google Calendar. The main content area displays the Altura Credit Union website. The site features a navigation menu with categories like PERSONAL, BUSINESS, EDUCATION, and ONLINE SERVICES. A prominent banner advertises "Want \$100 for something you already need to do?" with a "Learn" button. Other sections include "UPCOMING WORKSHOPS" with details for a "Retirement Planning Workshop" and a "Free Retirement Financial Planning Seminar in Hemet". A "YOU'RE PROTECTED" security notice is visible on the left side of the page.



Website Auto Complete

- *Do not* save passwords or other vital information in web browsers - it can be retrieved by viruses or someone that knows what they are doing.
- Use a password manager instead.
- For a free and secure password manager, check out <http://lastpass.com>.



Firewalls



- A firewall is a dedicated appliance or software that inspects network traffic passing through it and denies or permits passage based on a set of rules.
- What?



Firewalls



Simple example:

- Not using a firewall is like having a house with 65,000 doors and windows and leaving them all open. The house is open to infestation by pests (malware).
- Using a firewall is like having all the windows and doors closed with a guard monitoring who enters and exits from approved locations.

Firewalls



- One-way firewalls control incoming traffic from the internet, but not traffic leaving your computer (outgoing).
- Two-way firewalls control both incoming and outgoing traffic.
- Two-way firewalls may be the safest option, but they can be too complicated for the average user.

Firewalls



- There are hardware and software based firewalls.
- A hardware firewall is your typical router. These are excellent firewalls that can protect all computers on the network and they are more difficult to defeat than software based firewalls.
- A software firewall is a program that controls traffic to and from the internet.

Wireless Networks



- Wireless networks need to be secure!
- An unprotected wireless network allows anyone to access your network and possibly your computers. 
- This could have police knocking on your door because of what someone else was doing online. This is because a criminal could be committing online fraud from your internet account.



Extra Safety Measures

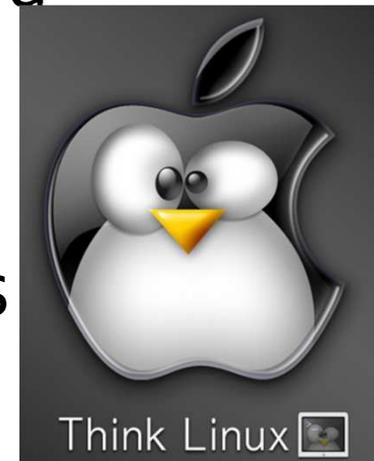
- Consider using a web browser other than Internet Explorer. The majority of people use Internet Explorer so many threats are engineered to exploit its vulnerabilities.
- Consider using the Google Chrome or Mozilla Firefox web browsers.
- Consider using a “secure” computer for online banking or other sensitive use. This type of system is up-to-date, not exposed to “risky” web browsing, and running a *quality* antivirus program.





Extra Safety Measures

- You can take an old computer and install the free Linux operating system. Linux is far less susceptible to viruses than the Windows operating system. Linux can run quite nicely on a computer that ran poorly with Windows XP.
- Apple is also a good option, but it has seen a spike in viruses lately.





Phishing and Online Fraud



Phishing



- Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
- Phishing is an example of social engineering techniques used to fool users.
- Phishing is typically carried out by email and often directs users to enter details at a fraudulent website that is made to look very much like the real thing.

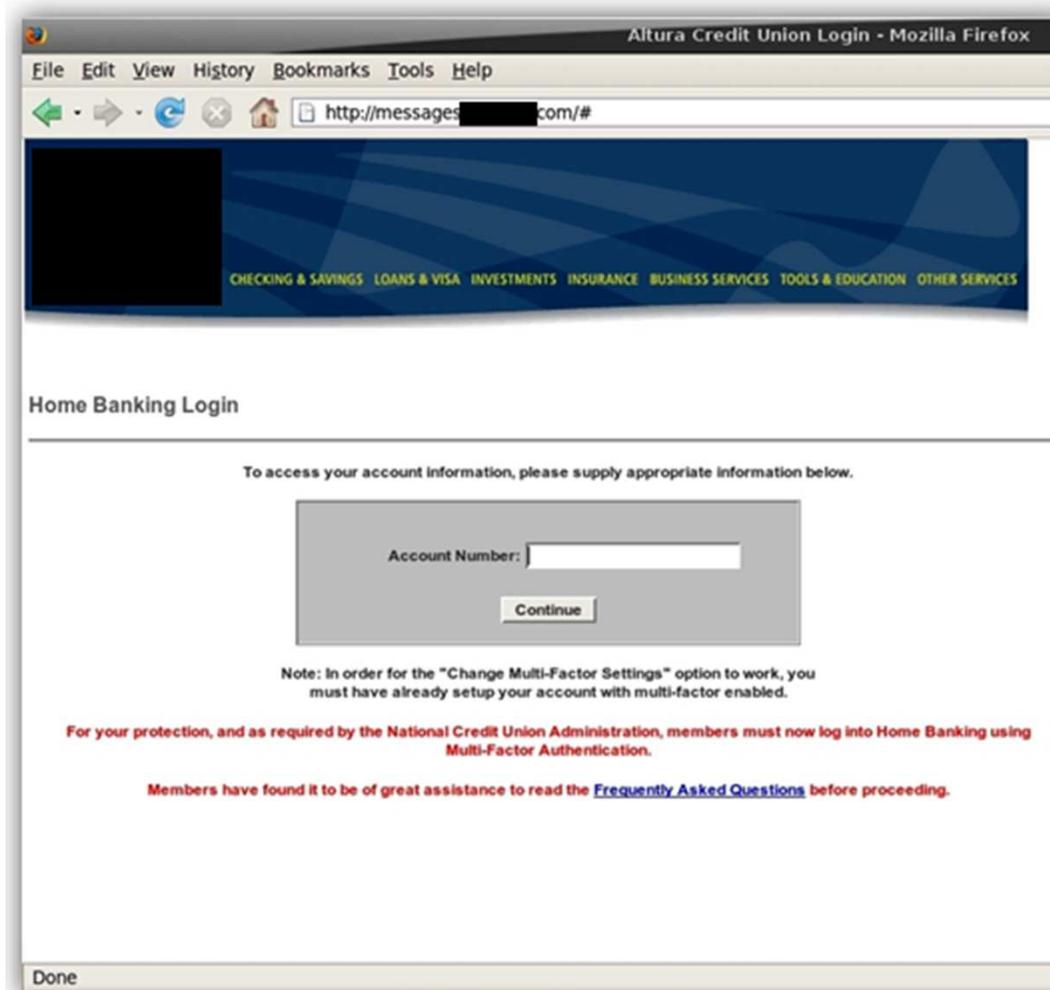


Credit Union Phishing Scam

- The following was a real phishing scam that targeted local Credit Union members. The phishing email provided a link that took victims to a legitimate looking website...



Credit Union Phishing Scam





Credit Union Phishing Scam

- Note that the website did not begin with https. (*It is not visible in the slide, but there was also no padlock.*)
- This web page should be secure since you would be transferring sensitive information (*your account number*).
- What happened when a victim entered their account number?



Credit Union Phishing Scam

Security Measures

Your Internet Banking Account is currently locked. Please enter your personal information below.
After you have filled in the necessary data, press the "Submit" button at the bottom of the page.

Full Name	<input type="text"/>
E-mail address	<input type="text"/>
Zip Code	<input type="text"/>
16 Digits Debit Card Number	<input type="text"/>
Debit Card Exp. Date	Month <input type="text"/> Year <input type="text"/>
Debit Card Cvv2	<input type="text"/>
4 Digits Debit Card ATM PIN (REMEMBER! This is not the password you use to login)	<input type="text"/> Personal Identification Number you use at ATM machine
Verify Debit Card ATM PIN	<input type="text"/>



Credit Union Phishing Scam

- After a victim entered their vital information and pressed submit, the information was most likely sent to waiting criminals.
- Who will arrest the criminals if they are in China, Russia, Nigeria, etc.?



Other Online Fraud

- You receive an email from a friend saying they are on vacation, they got mugged, and they need money. Call your friend before sending money.
- You receive an email from a stranger saying they came into a large amount of money and they need you to help get it into the United States. If it sound too good to be true, it probably is...

Confidence Scams

- This is one of the lowest forms of fraud because the suspects locate vulnerable victims on social or dating sites.
- Suspects “romance” the victims and gain their trust before asking for money.
- Suspects keep asking for more and more until the victim finally catches on or is broke...
- Many of these scams originate out of the country and therefore are out of our reach.



Unsure About an Email?

- If you get an email about a problem with your account - call the bank or go to the [real] website, but **DO NOT CLICK ON A LINK IN AN EMAIL!**
- Once logged on to your account, you should be able to see if you have any alerts.
- The bank might also address bogus emails on their main page.



Go Arrest these Criminals!

- This is not as simple as arresting a local criminal.
- There are jurisdictional issues because many cyber criminals are not in the United States.
- If a criminal knows what they are doing they may never be caught because there are ways of staying totally anonymous online.



Sexual Predators

TRACKING ON-LINE PREDATORS

**TROY
HELM**

**CHARGED WITH
INTERNET STALKING
OF A CHILD, CRIMINAL
INTENT TO COMMIT
RAPE**



**FOX
16**



Sexual Predators

- A sexual predator can be anyone they choose while online. A 40 year old male can be a 15 year old boy or girl while online.
- The world wide web has become one of the biggest social gathering places. Sexual predators no longer need to loiter around parks to stalk children. They merely need to go to any social networking site or chat room kids use.



Sexual Predators

- To Catch a Predator is a series that exposes online sexual predators. It's an eye opener...





Monitor Kids

- Kids are targets for sexual predators.
- They will download anything.
- Consider not allowing children to have a computer in their bedroom or other location where you cannot monitor them.
- If you do allow a child to have a computer in a private location, consider restricting access to the internet.



Monitor Kids

- There are systems to prevent access to adult or risky sites. Check out www.opendns.com.
- There are also programs to secretly monitor online activities.



Record all their Emails, Chats, Keystrokes and Web Sites Visited

As a parent you want to provide Internet access as an outlet for your child to thrive, however their safety is your highest priority. The Internet is full of danger that an unsuspecting and innocent child may overlook. For instance, social networking web sites such as Facebook and MySpace are a great outlet

"Your product saved my son's life and turned it around! I will never stop telling others about your product."

D. Wise - Chicago, IL

We're Available 24/7
1.877.288.5702

SpectorSoft's U.S.-based representatives are available 24 hours a day, 7 days a week to answer your technical questions or complete your purchase by phone.



Monitor Kids

- If your children have social networking accounts, it is a good idea to look at them from time to time. It is shocking what kids (and adults) will put on the web.
- Check with online safety websites for more in-depth information on protecting children and recommended software.

<http://www.wiredsafety.org/>



Resources

- Ubuntu Linux: <http://www.ubuntu.com/>
- Megan's Law Website: <http://www.meganslaw.ca.gov/>
- Perverted Justice: <http://www.perverted-justice.com/>
- Online Safety Information: <http://www.wiredsafety.org/>
- To Catch a Predator: <http://www.msnbc.msn.com/id/10912603/>
- Security Watch: <http://blogs.pcmag.com/securitywatch/>
- NOD32 Antivirus: <http://www.eset.com/home>
- Kaspersky Antivirus: <http://usa.kaspersky.com/>
- Microsoft Security Essentials Antivirus: http://www.microsoft.com/security_essentials/
- LastPass Password Manager: <https://lastpass.com/>
- Malwarebytes Antimalware: <http://www.malwarebytes.org/mbam.php>
- Firefox Web Browser: <http://www.mozilla.com/en-US/firefox/>
- Google Chrome Web Browser: <http://www.google.com/chrome/>
- Microsoft Update: <http://www.update.microsoft.com/>
- Spector Pro: <http://www.spectorsoft.com/spectorproiswatching.asp#>
- Spoofing Attack: http://en.wikipedia.org/wiki/Spoofing_attack
- Internet Crime Complaint Center: <http://www.ic3.gov/default.aspx>