



Test Your Tech

Crackers and cookies are:

- A. Bytes to share with friends.
- B. The best minor league baseball team of all time and their cheerleaders.
- C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).



Test Your Tech

Crackers and cookies are:

- A. Bytes to share with friends.
- B. The best minor league baseball team of all time and their cheerleaders.
- C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).



Security

Exploring the Dark Side of the
Internet



Negative Issues

- Malware
 - * Viruses, et al.
 - * Spyware / Adware
- Privacy
 - * Phishing
- Malicious
 - * Cracking (not hacking)
 - * Network service attacks



Different Types of Virii/Spyware

- Spyware
- Adware
- Embedded Programs
- Trojan Horse
- Browser Hijackers
- Dialers
- Worms



Why do people make Virii/Spyware?

- Profit
- Malice
- Boredom
- Business
- A challenge
- "Respect" from other virii writers



How do I know if I've got a Virus/Spyware?

- Virii
 - * Programs will stop working correctly
 - * Loosing data (documents disappearing)
 - * Computer is running slower than normal
- Spyware
 - * Popups (on or off the internet)
 - * New toolbars
 - * Home page changes
 - * Search results look different
 - * Error messages when accessing the web



What does Spyware look like?





What does Spyware look like?





What does Spyware look like?

Are you being spied on?

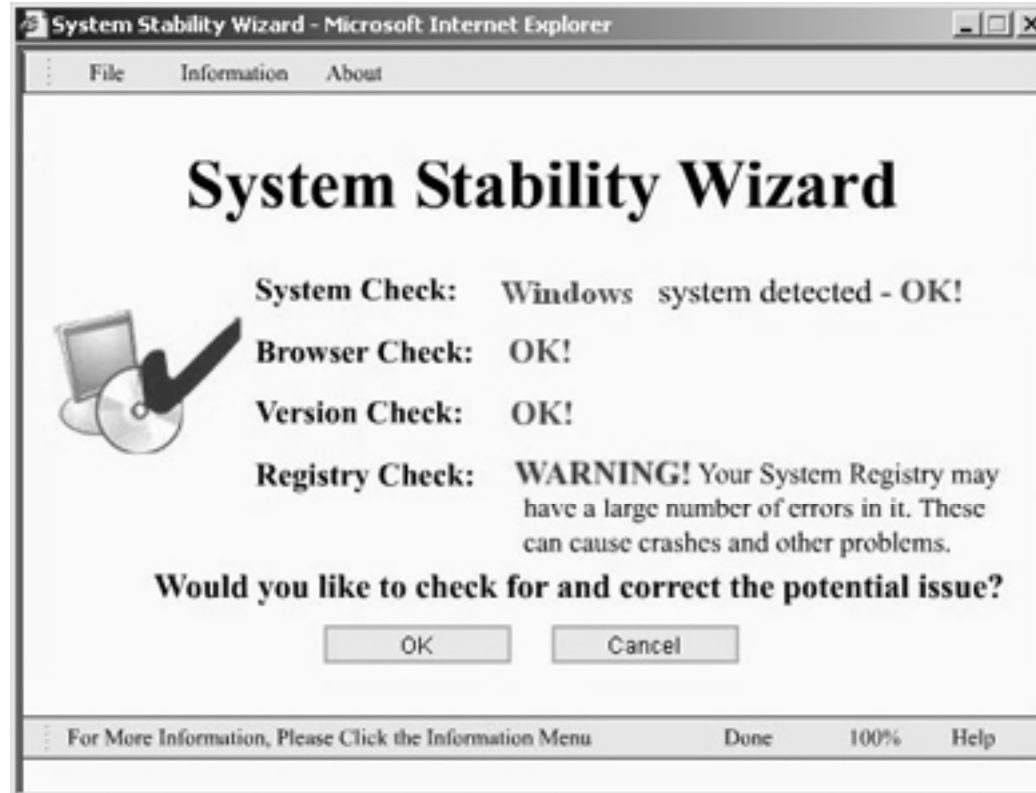
Internet thieves watch and record your personal and private information, even the websites you visit, without you ever knowing. Fight back! Find out who is spying on you.

FREE Spyware Scan

FREE scan compliments of AluriaSoftware™



What does Spyware look like?



What does Spyware look like?



Special Discounts and Offers - Microsoft Internet Explorer

VEGAS CASINO ONLINE
Online Since 1999

THE BIGGEST BONUS ON THE NET!
2 Easy Steps
Enter Email & Click Download Now
Collect Your
200% Bonus!

Enter your E-mail Here

Download Casino Now

- 200% Bonus for New Players
- Fast & Easy Download
- Cutting-Edge Software
- Play For Fun Or For Real
- Better Than Vegas Odds
- Completely Safe & Secure
- Fast Payouts

CARD GAMES TABLE GAMES PROGRESSIVE GAMES

MORE GAMES MORE GAMES MORE GAMES

Play For Real

Done Internet



What does Spyware look like?



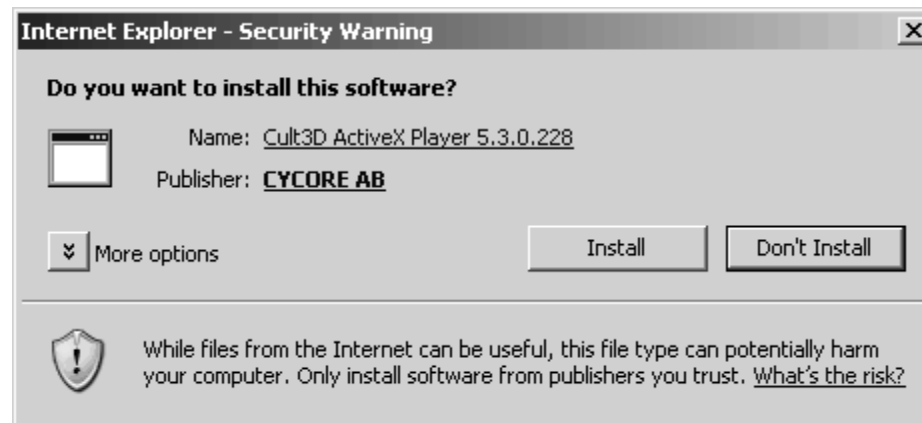


What does Spyware look like?



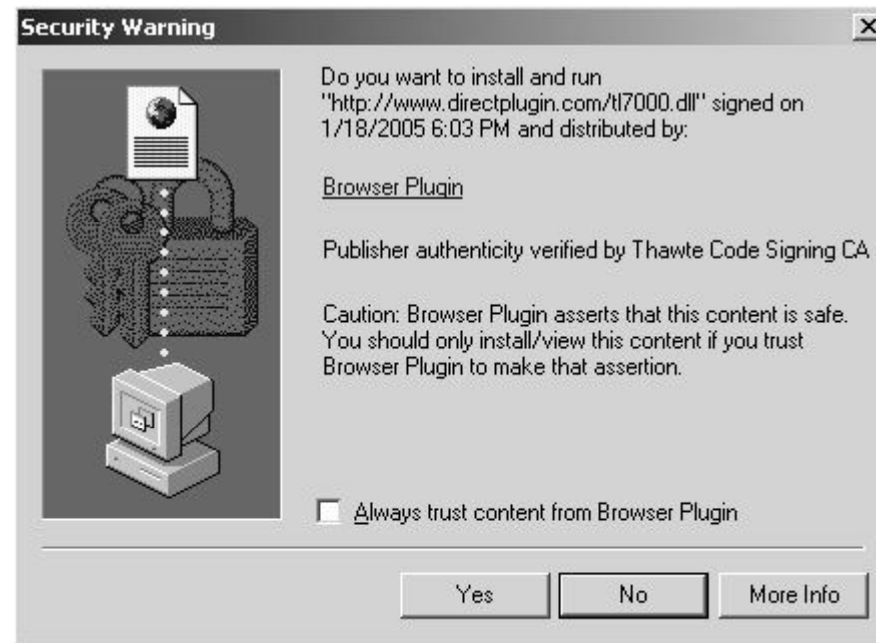


What does Spyware look like?



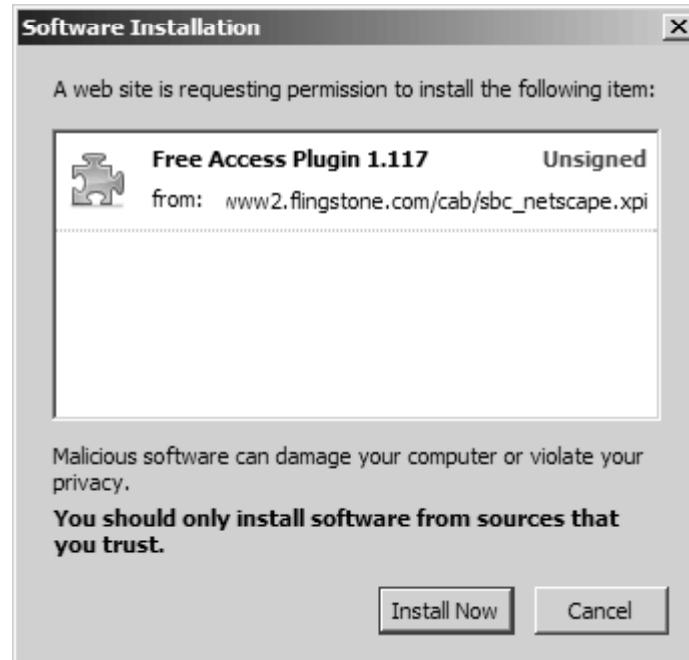


What does Spyware look like?





What does Spyware look like?





How do I get rid of Spyware?

- Use a *legitimate* spyware removal program
 - * Windows Defender:
<http://www.microsoft.com/athome/security/spyware/software/>
 - * Spybot:
<http://www.safer-networking.org/en/>



How do I prevent Spyware?

- Be conscious of what you are clicking on/downloading
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it. Always look for the topmost right red X.
- Remember that things on the internet are rarely free. "Free" Screensavers etc. generally contain ads or worse that pay the programmer for their time.



How do I get rid of/prevent Virri?

- Run antivirus software
 - * <http://www.washington.edu/computing/security>
- Keep it up to date!
 - * Virus definitions need to be updated regularly!



Phishing

- Most commonly an Email stating your account information needs updating
- Watch for URL's that are numeric or different from the link you clicked on
- Best thing to do is to type in the URL and check your account directly without following any links in the Email
- Many legitimate emails no longer contain a link (Paypal)



Phishing Examples

Receipt for Your Payment to phonebuyer - Cyrillic (Windows)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: PayPal
Date: Saturday, October 23, 2004 11:15 PM
To: none
Subject: Receipt for Your Payment to phonebuyer

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

This email confirms that you have paid phonebuyer (phonebuyer451@yahoo.com) \$278.99 USD using PayPal.

Payment Details

Item #	Item Title	Quantity	Price	Subtotal
8126628705	<u>Myst III</u>	1	\$270. USD	\$270.00 USD

Shipping & Handling via USPS First Class Mail \$8.99 USD
(includes any seller handling fees)

Shipping Insurance (not offered) : --

Total: \$278.99
USD

If you did not authorize this payment or if you need assistance with your account, please contact PayPal customer service at:

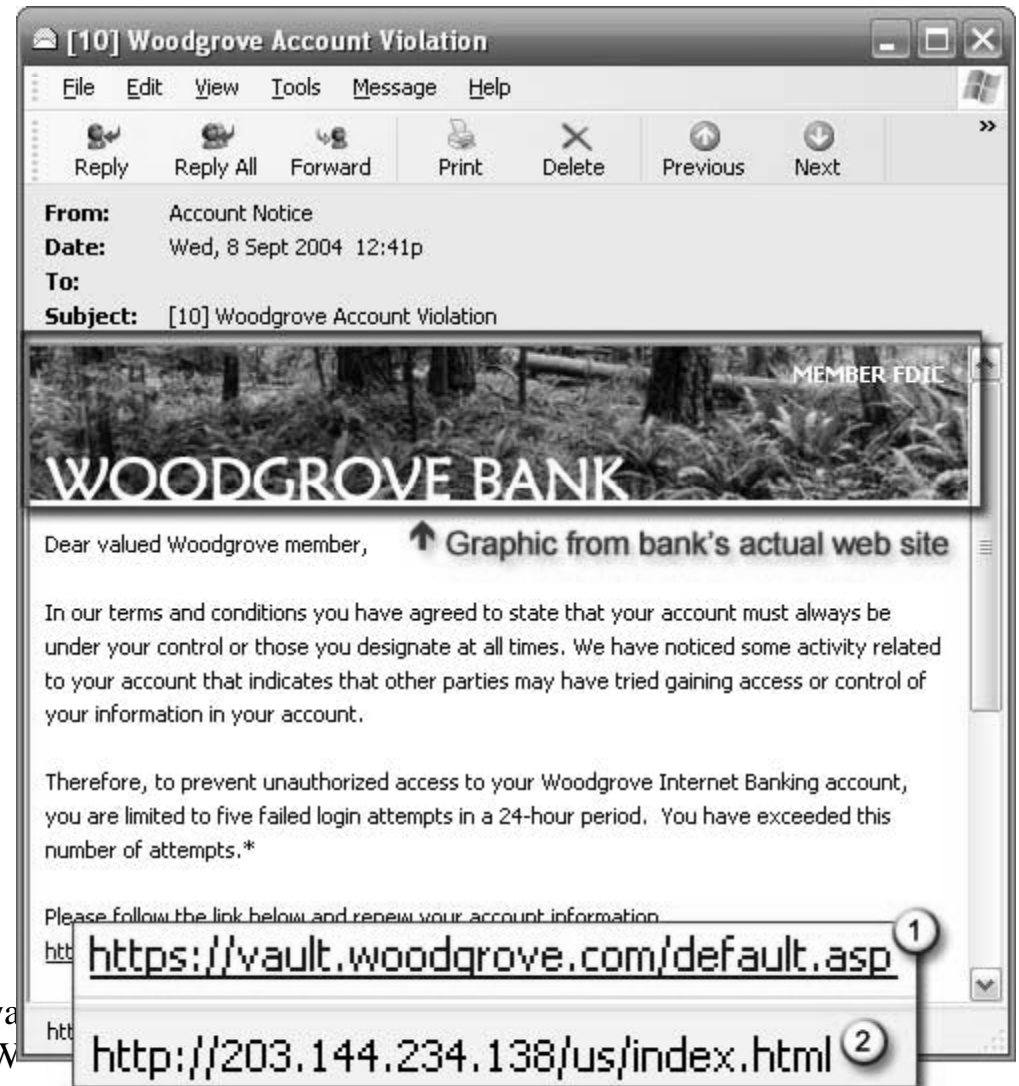
<https://www.paypal.com/row/wf/f=payment-fraud>

<http://paypalpro.us/hou>

fit100-21-



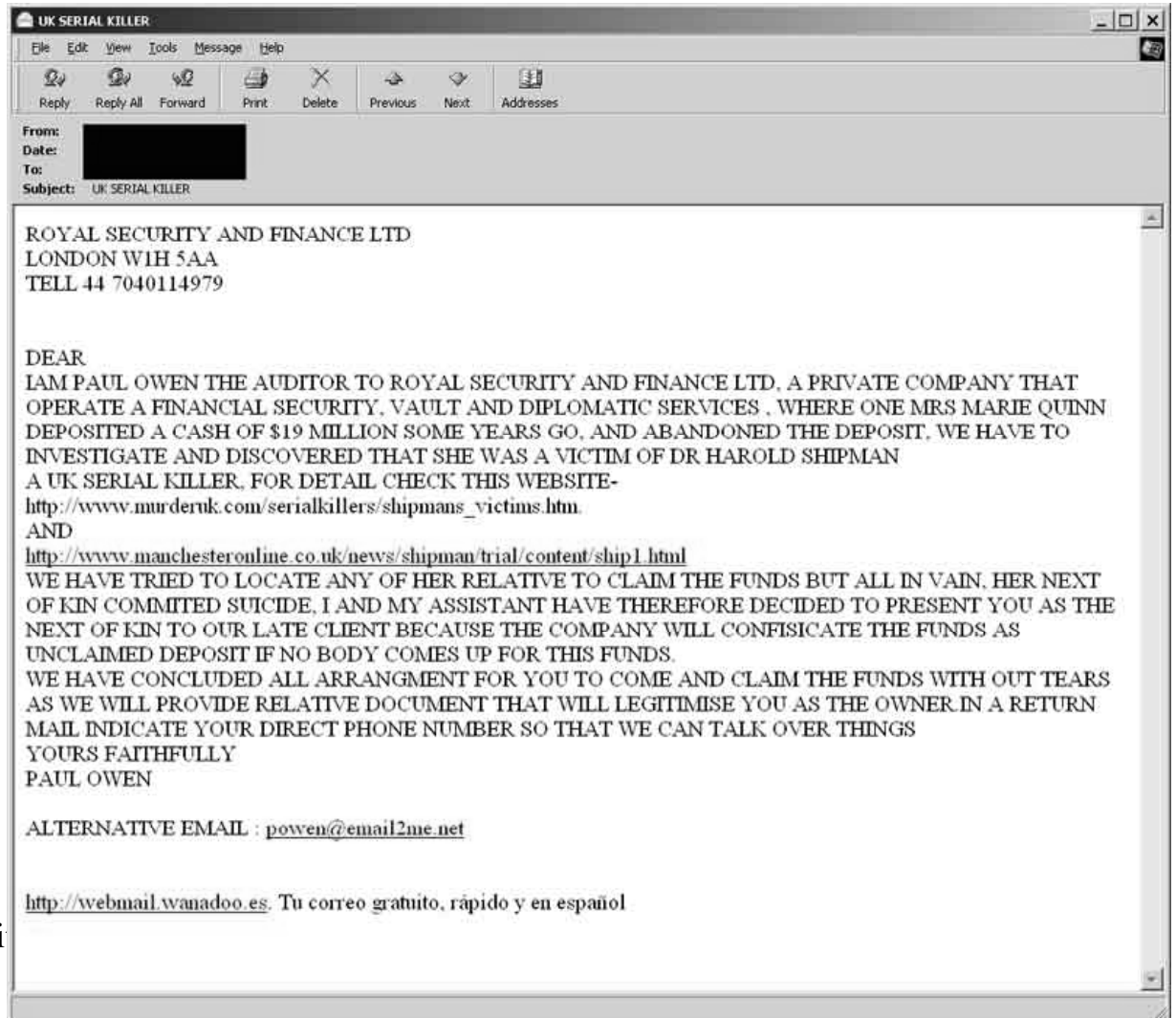
Phishing Examples



fit100-21-spywa
of W



Phishing Examples



fi



Phishing Examples



Dear US Bank Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
http://www.usbank.com/internetBankin_g/RequestRouter?requestCmdId=DisplayLoginPage

Note: Requests for information will be initiated by US Bank Business Development, this process cannot be externally requested through Customer Support.

Sincerely,
US Bank Accounts Department.

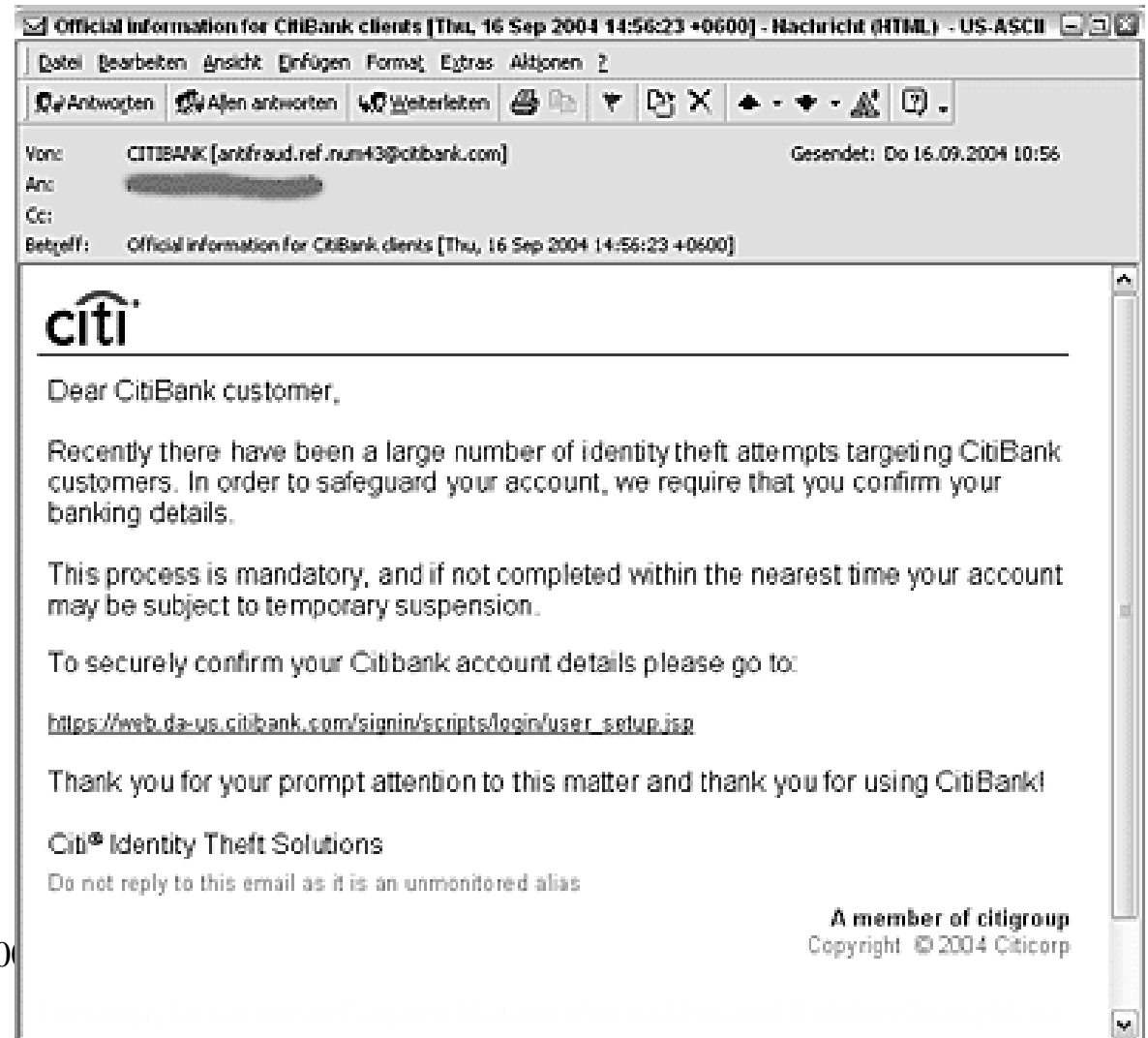
Summary | Next | Reply | Reply All | Forward | Delete

<http://testme.3322.org/faq/bin/index.html>

Internet



Phishing Examples



fit100




Phishing Examples

TKO NOTICE: eBay request, please read - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

X To protect your privacy, Thunderbird has blocked remote images in this message. Show Images


Subject: TKO NOTICE: eBay request, please read **From:** aw-confirm@ebay.com 29.09.2004 14:58


 **Update Your Account Information Within 24 Hours**

Valued eBay Member,

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be suspended within 24 hours for investigations.

Never share your eBay password to anyone!

Establish your proof of identity with ID Verify (free of charge) - an easy way to help others trust you as their trading partner. The process takes about 5 minutes to complete and involves updating your eBay information. When you're successfully verified, you will receive an ID Verify icon  in your feedback profile. Currently, the service is only available to residents of the United States and U.S. territories (Puerto Rico, US Virgin Islands and Guam.)



To update your eBay records [Click here:](#)

<http://202.149.196.236/.aw-cgicgisk/SignIn.php>



How secure do you
need to be?

- Be Prudent not Paranoid
- Did you initiate the action?
- Why is this free?
- Is the source trustworthy?
- When in doubt search for it!



- White Hat

- * Very tech savvy and use powers for good
- * Security consulting, penetration testing, security audits, etc...
- * Goal is to help

- Grey Hat

- * Very tech savvy and use powers for good - sort of
- * Goal is often to help, but by doing mischievous things in the process

- Black Hat

- * Very tech savvy
- * The bad guy!
- * Goal is to "own you"

Hackers



Cracking (Bad Hacking)

- Black Hats doing bad things
 - * Defacing web sites
 - * Stealing private information
 - * Stealing money
 - * Blackmail
 - * Etc...



Cracking - What are their secrets?

- Social Engineering
 - * Manipulating people to have them give you access
 - * "Hello I am calling from tech support about the problem you submitted. Let me get your password and I will help you right away..."
- Buffer Overflow
 - * Finding problems in programming code
 - * Writing outside of memory location (Example - writing past the end of an array into a variable called: myPassword and saving your own password)
- Cross Site Scripting
 - * One site or program is used to edit another site
 - * See my example:
<https://faculty.washington.edu/samspade/secure/> (works in IE and Safari)



Denial of Service Attack

- Also known as a DoS attack
 - * attack on a computer system or network that causes a loss of service to users
- Consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
- Sort of like someone constantly calling you over and over again. You wouldn't be able to use your phone.
- If they don't affect you directly
 - * May slow down your network service...
- If they do affect you directly
 - * May block your network service...



Questions

- If I wanted to update a group of co-workers about a project and solicit their feedback, would I want to use a synchronous or asynchronous system?
- What communication system would work well and why?



Questions

- If I were in marketing, and wanted to “put my finger on the pulse” of a particular group of people: say candy lovers, what social technologies could I use to find out what they are thinking?