


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).

1




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).

2



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


fit100-21-spyware © 2008 University of Washington



Different Types of Virii/Spyware

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


fit100-21-spyware © 2008 University of Washington



Why do people make Virii/Spyware?

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


fit100-21-spyware © 2008 University of Washington




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


fit100-21-spyware © 2008 University of Washington




What does Spyware look like?



fit100-21-spyware © 2008 University of Washington



What does Spyware look like?




fit100-21-spyware © 2008 University of Washington




What does Spyware look like?



fit100-21-spyware © 2008 University of Washington



What does Spyware look like?




fit100-21-spyware © 2008 University of Washington




What does Spyware look like?





of Washington

 What does Spyware look like?





fit100-21-spyware © 2008 University of Washington

 What does Spyware look like?





fit100-21-spyware © 2008 University of Washington

 What does Spyware look like?




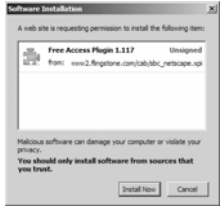
fit100-21-spyware © 2008 University of Washington

 What does Spyware look like?




fit100-21-spyware © 2008 University of Washington

 What does Spyware look like?




fit100-21-spyware © 2008 University of Washington

 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/>


fit100-21-spyware © 2008 University of Washington



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.


fit100-21-spyware © 2008 University of Washington



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!


fit100-21-spyware © 2008 University of Washington



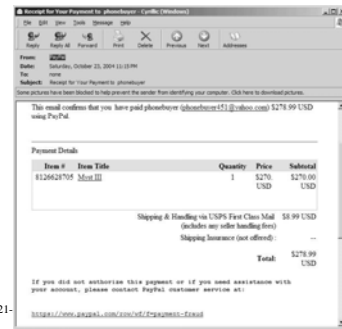
Phishing

- 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)

fit100-21-spyware © 2008 University of Washington




Phishing Examples

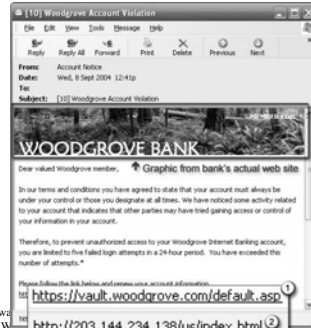


Item #	Item Title	Quantity	Price	Subtotal
8126423705	Mon III	1	\$276.00 USD	\$276.00 USD
Shipping & Handling via USPS First Class Mail (includes any sales handling fees)				\$8.99 USD
Shipping Insurance (not offered):				--
			Total:	\$276.99 USD


fit100-21-
<http://www.paypal.com/web/WebPage1-Fraud>




Phishing Examples




fit100-21-spyware of W




Phishing Examples



fit



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/InternetBanking/UpdateAccountInformation.aspx>

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



Phishing Examples



Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.


This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your CitiBank account details please go to:
https://web.fis.us.citibank.com/online/securelogin/secure_login.asp


Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions
Do not reply to this email as it is an unmonitored alias

A member of Citigroup
 Copyright © 2004 Citicorp



Phishing Examples



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 account click here



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!


fit100-21-spyware © 2008 University of Washington



Hackers

- 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"

fit100-21-spyware © 2008 University of Washington



Cracking (Bad Hacking)

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

fit100-21-spyware © 2008 University of Washington



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/sampade/se-cure/> (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...

fit100-21-spyware © 2008 University of Washington



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?

fit100-21-spyware © 2008 University of Washington