

## 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



Special Offer From Callwave

Registry Cleaner Recommended

Errors in your Windows registry database, if present, could cause erratic operation and other computer problems, including:

\* Slow system performance

\* Slow system performance

\* Slow system crashes

Details:

To ensure that your system is operating correctly, we strongly recommend you scan and clean your Windows registry database by running Registry Cleaner now.

To download Registry Cleaner and scan for errors, click "Scan and Clean":

Scan and Clean

All information in this advertisement for free Registry Cleaner software courtesy SoftwareOnline.com. No system check yet performed or implied.
From time-to-time, CallWave will display advertisements from select partner companies. To update your settings, features, or to check-out other

fit100-21-spyware © 2008 University of Washington

service levels (without ads), please click here











File	Information About					
	System Sta	ability Wizard				
	System Check:	Windows system detected - OK!				
A	Browser Check:	OK!				
	Version Check:	OK!				
	Registry Check:	WARNING! Your System Registry may have a large number of errors in it. These can cause crashes and other problems.				
١	Would you like to check	k for and correct the potential issue?				
	OK	Cancel				
	nformation, Please Click the Inform	ution Menu Done 100% Help				



of Washington







	Easy	in the law - Heat - Heat - Among -	hoo®
Welcome	Easy Messenger	AIM®	MSN
Easy Messenger le one convenient l	ets you combine your AIM®, MSI M!	N®, Yahoo®, and ICQ® be	uddies into
	owered by 180search Assistant, a pro and helps keep online entertainmen Assistant can be accessed from an icc	nt and downloads free and s on in your system tray. This	safe. When
	ge of 2-3 keyword-based advertiser v	web pages daily.	
shows you an averag			agreement



Internet	Explorer - Security Warning	×
Do you	u want to install this software?	
	Name: <u>Cult3D ActiveX Player 5.3.0.228</u> Publisher: <u>CYCORE AB</u>	
× Mo	ore options Install Don'	't Install
1	While files from the Internet can be useful, this file type can potential your computer. Only install software from publishers you trust. What	











# How do I get rid of Spyware?

- Use a *legitimate* spyware removal program
  - \* Windows Defender: <u>http://www.microsoft.com/athome/se</u> <u>curity/spyware/software/</u>

\* Spybot: <u>http://www.safer-networking.org/en/</u>



# 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
  - \* <u>http://www.washington.edu/computin</u> <u>g/security</u>
- Keep it up to date!
  - \* Virus definitions need to be updated regularly!



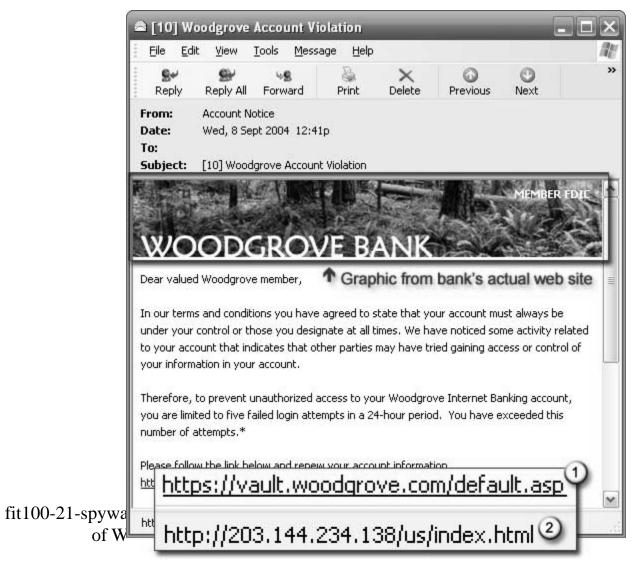
# Phishing

- 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)



🚔 Receipt for Your Payment t	phonebuyer - Cyrillic	(Windows)				
<u>File E</u> dit <u>V</u> iew <u>T</u> ools <u>M</u> e	ssage <u>H</u> elp			(c		
Reply Reply All Forward	Print Delete	Previous	(V) Next	M Addresses		
From: PayPal Date: Saturday, October 2: To: none Subject: Receipt for Your Pay						
Some pictures have been blocked to	help prevent the sender f	from identifying	your comp	uter. Click her	e to downloa	ad pictures.
This email confirms that using PayPal.  Payment Details	you have paid phon	couyer (pilo	neouyer-		<u></u> , 32	
Item # Item T	itle			Quantity	Price	Subtotal
8126628705 <u>Myst I</u>	I			1	\$270. USD	\$270.00 USD
	Shippin	g & Handlin (incl	-	PS First Cl seller hand		\$8.99 USD
		Ship	ping Insu	rance (not	offered) :	
					Total:	\$278.99 USD
If you did not au your account, plea					stance w	rith
https://www.paypa	.com/row/wf/f=pa	ayment-fra	aud			
http://paypalpro.us/nou						







20	Q,	1000 CT		V	- 76	10.0	60
Reply		₩ <u>2</u> Forward	Print	Delete	Previous	< ≫ Next	Addresses
From: Date: To: Subject:	uk serial	KILLER					
LONI TELL DEAF IAM I OPER DEPC INVE	ATE A STIGAT	FINAN A CASI TE AND	HE AU CIAL S H OF \$1 DISCO	DITOR ECURI 19 MILI IVEREI	TO RO' IY, VAU JON SC D THAT	JLT AD ME Y SHE	ECURITY AND FINANCE LTD, A PRIVATE COMPANY THAT ND DIPLOMATIC SERVICES , WHERE ONE MRS MARIE QUINN EARS GO, AND ABANDONED THE DEPOSIT, WE HAVE TO WAS A VICTIM OF DR HAROLD SHIPMAN
							IIS WEBSITE-
http:/// AND http:/// WE H OF KI NEXT UNCI WE H AS W MAIL YOU	WWW.m AVE TI N COM OF KI AIMEI AVE CO E WILL INDIC.	anchesta RIED TO MITED N TO O DEPO: ONCLU PROVI ATE YO HFULL	com/se con/se coloc/ suici ur LA SIT IF 1 DED A DE REI OUR DI	rialkille <u>co.uk/i</u> ATE AN DE, I AJ FE CLIE NO BOI LL ARF LATIVE	ers/shipr news/shi IY OF H ND MY ENT BE OY COM CANGM E DOCU	nans_v pman/t ER RE ASSIS CAUSI (ES UI ENT F MENI	IIS WEBSITE- ictims.htm. ELATIVE TO CLAIM THE FUNDS BUT ALL IN VAIN, HER NEXT STANT HAVE THEREFORE DECIDED TO PRESENT YOU AS THE E THE COMPANY WILL CONFISICATE THE FUNDS AS P FOR THIS FUNDS. FOR YOU TO COME AND CLAIM THE FUNDS WITH OUT TEARS THAT WILL LEGITIMISE YOU AS THE OWNER IN A RETURN FER SO THAT WE CAN TALK OVER THINGS
http:/// AND http:/// WE H OF KI NEXT UNCI WE H AS W MAIL YOUH PAUL	WWW.B AVE TI N COM OF KI AIMET AVE CO E WILL INDIC. & FAII OWEN	underuk RIED T( IMITED N TO O DEPO: ONCLU: PROVI ATE YC HFULL	com/se eronline O LOCA SUICE UR LAT SIT IF 1 DED A DE RE DUR DE Y	rialkille co.uk/r ATE AN DE, I AI TE CLIE NO BOI LL ARF LATIVE RECT P	ers/shipr news/shi IY OF H ND MY ENT BE OY COM CANGM E DOCU	nans_v pman/t ER RE ASSIS CAUSI IES UI IES UI ENT F MENT NUMB	rictims.htm. <u>Arial/content/ship1.html</u> ELATIVE TO CLAIM THE FUNDS BUT ALL IN VAIN, HER NEXT STANT HAVE THEREFORE DECIDED TO PRESENT YOU AS THE E THE COMPANY WILL CONFISICATE THE FUNDS AS P FOR THIS FUNDS. FOR YOU TO COME AND CLAIM THE FUNDS WITH OUT TEARS THAT WILL LEGITIMISE YOU AS THE OWNER IN A RETURN





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.

Summane Nevt

Renty | Renty All | Forward | Delete

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



	en Ansicht Einfügen Format Egtras Aktjonen 2
Ø.≱Antworten	∰Ajen artworten 4@ Meterleten 🖉 ि 🔻 🕑 🗙 🔶 🔹 🔹 🌜 🕐 .
Von: CITI	84NK (antfraud.ref.num43@citbank.com) Gesendet: Do 16.09.2004 10:56
Ce:	
Betgelf: Offic	ial information for CitiBank clients [Thu, 16 Sep 2004 14:56:23 +0600]
citi	
Dear CitiE	Bank customer,
banking d This proce	a. In order to safeguard your account, we require that you confirm your etails. ass is mandatory, and if not completed within the nearest time your account ubject to temporary suspension.
To secure	ly confirm your Citibank account details please go to:
https://web.	da-us.citibank.com/signin/scripts/login/user_setup.jsg
Thank yo	u for your prompt attention to this matter and thank you for using CitiBank!
Citi@ Ideni	tity Theft Solutions
	to this email as it is an unmonitored alias
	to this email as it is an unmonitored alias A member of citigroup Copyright © 2004 Citicorp



4							
📽 TKO NOTICE: eBay request, please read - Mozilla Thunderbird							
<u>File Edit View Go Message Enigmail T</u> ools <u>H</u> elp							
🗙 To protect your privacy, Thunderbird has blocked remote images in th	is message.	Show Images					
<ul> <li>Subject: TKO NOTICE: eBay request, please read</li> </ul>	From: <u>aw-confirm@ebay.com</u>	29.09.2004 14:58					
Update Your Account Information Within 2	4 Hours						
Valued eBay Member,							
According to our site policy you will have to confirm that you a completing the following form or else your account will be susp		,					
Never share your eBay password to anyone!							
Establish your proof of identity with ID Verify (free of charge) trading partner. The process takes about 5 minutes to complex When you're successfully verified, you will receive an ID Verify service is only available to residents of the United States and and Guam.)	te and involves updating your e icon 왕 in your feedback profile	Bay information. e. Currently, the					
CONTRACTOR Click here:							

To update your eBay records <u>Click here</u>:

-()= 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

## Hackers

- \* 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"



# 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: <u>https://faculty?-washingponiedu/samspade/se</u> 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



### Questions

- If I wanted to update a group of coworkers 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?