Computer Security

David Wagner, C79, 4/4/2013

themes so far:

- measuring risk

- cognitive biases

- probability reduction (e.g., vaccines)

- harm reduction (e.g., treatment)

themes so far:

- measuring risk

- cognitive biases

- probability reduction (e.g., vaccines)

- harm reduction (e.g., treatment)

today: dealing with uncertain risks

computer security is immature

botnet	% of spam	new spam/day	new spam/ min	spam / bot/min	estimated botnet size	Country of Infection
Rustock	19%	20,191,511,739	14,021,883	91	540k to 810k	Brazil (21%), USA (9%), Poland (7%)
Cutwail	17%	18,417,396,993	12,789,859	59	1100k to 1600k	Vietnam (17%), RepKorea(12%), Braz
Bagle	16%	17,334,321,383	12,037,723	37	520k to 780k	Brazil (12%), Spain (9%), USA (9%)
Bobax	14%	14,589,066,047	10,131,296	49	100k to 160k	Spain (12%), Italy (7%), India (7%)
Grum	9%	9,687,625,087	6,727,517	307	580k to 860k	Vietnam (18%), Russia (17%), Ukraine
Maazben	2%	2,161,829,037	1,501,270	93	240k to 360k	Romania (17%), Brazil (11%), Saudi A
Festi	1%	1,353,086,645	939,644	53	140k to 220k	Vietnam (31%), India (11%), China (5%
Mega-D	1%	996,079,588	691,722	46	50k to 70k	Vietnam (14%), Brazil (11%), India (6%
Xarvester	1%	885,682,360	615,057	155	20k to 36k	Brazil (15%), Poland (11%), USA (10%
Gheg	0%	436,044,470	302,809	22	50k to 70k	Brazil (15%), Poland (8%), Vietnam (8
Unclassified Botnets	3%	2,994,054,378	2,079,204	65	120k to 180k	
Other, smaller botnets	0%	439,986,486	305,546	47	130k to 190k	
Total BotnetSpam	**83%**	**89,486,684,212**	62,143,531	**85**	**3600k to 5400k**	**Brazil (13%), Vietnam (7%), USA (6%**
Non-botnet spam	**17%**	**17,827,092,771**	12,379,926			
Grand Total	**100%**	**107,313,776,983**	74,523,456			

MessageLabs

SYMANTEC HOSTED SERVICES™

traditional view:

computer security is risk management

This kind of counterintuitive security is common in the world of gemstones. On 47th Street in New York, in Antwerp, in London: People walk around all the time with millions of dollars' worth of gems in their pockets. The gemstone industry has formal guidelines: If the value of the package is under a specific amount, use the U.S. Mail. If it is over that amount but under another amount, use Federal Express. The Cullinan was again transported incognito; the British

MANUAL

DOE M 470.4-1

Approved: 8-26-05
Review: 8-26-07
Chg 1: 3-7-06

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

U.S. DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

Vertical line denotes change.

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		

Department of Energy
Washington, DC 20585

August 7, 2006

MEMORANDUM FOR: ASSOCIATE DIRECTORS
OFFICE DIRECTORS
SITE OFFICE MANAGERS

FROM: GEORGE MALOSH
ACTING CHIEF OPERATING OFFICER
OFFICE OF SCIENCE

SUBJECT: Office of Science Policy on the Protection of Personally Identifiable Information

The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing

- **Incident Reporting**

Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

Vast Data Cache About Veterans Is Stolen

By DAVID STOUT and TOM ZELLER Jr.
Published: May 23, 2006

WASHINGTON, May 22 — Personal electronic information on up to 26.5 million military veterans, including their Social Security numbers and birth dates, was stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization, the agency said Monday.

Called to account at Capitol Hill hearings, Nicholson said he was angry that he hadn't been told about the burglary until nearly two weeks after it happened.

The theft exposed lax data-security procedures at the agency and led to congressional hearings and the departures of five senior VA officials. It also appears to have ended Johnson's career:

Rapiscan
DANGER RADIATION
C48
A77
250 CITIES
50 COUNTRIES

traditional view:

computer security is risk management

$$\text{risk} = E[\text{loss}] = P(\text{breach}) \times \text{cost}(\text{breach})$$

$$\text{risk} = E[\text{loss}] = P(\text{breach}) \times \text{cost}(\text{breach})$$

often not known

risk = E[loss] = P(breach) × cost(breach)

often not known

does the system have a vulnerability?

risk = E[loss] = P(breach) × cost(breach)

often not known

does the system have a vulnerability?

will attackers exploit it?

1 million lines of code

1 million lines of code

× 1 bug / thousand lines of code

1 million lines of code

× 1 bug / thousand lines of code

= 1000 bugs

1 million lines of code

× 1 bug / thousand lines of code

= 1000 bugs

attacker only needs to find 1 bug;
defender must find all of them

1 million lines of code

× 1 bug / thousand lines of code

= 1000 bugs

attacker only needs to find 1 bug;
defender must find all of them

don’t know whether system is vulnerable

attackers choose how and whether to attack

attackers choose how and whether to attack

attacks change rapidly

attackers choose how and whether to attack

attacks change rapidly

no good data about prob. of breach

$$\text{risk} = E[\text{loss}] = P(\text{breach}) \times \text{cost}(\text{breach})$$

often not known

implications

security market is sometimes dysfunctional

market for lemons

thinking about risks,
when there are multiple players

CHASE
Bank of America
WELLS
FARGO

US banks spent less on security
but fraud rates higher in UK

UK:

US:

US banks spent less on security
but fraud rates higher in UK

UK: liability for fraud on customer

US:

US banks spent less on security
but fraud rates higher in UK

UK: liability for fraud on customer

US: liability for fraud on bank

US banks spent less on security
but fraud rates higher in UK

UK: liability for fraud on customer

US: liability for fraud on bank

huh?

US banks spent less on security
but fraud rates higher in UK

UK:

US:

UK: fraud? you must have been careless.
tough luck, sucks to be you

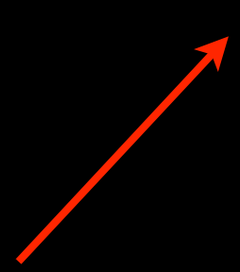
US:

UK: fraud? you must have been careless.
tough luck, sucks to be you

US: fraud? no problem, we'll reimburse you

UK: fraud? you must have been careless.
tough luck, sucks to be you

US: fraud? no problem, we'll reimburse you



good for customers, but also
good for banks

moral hazard

UK banks got lazy and careless,
leading to an epidemic of fraud

lesson:

align incentives

rule of thumb:
place liability on whoever is in the best position to do something about it

externalities

spam

spam

~ 90% of all email is spam

spam

~ 90% of all email is spam

costs US $20 billion per year,
in lost productivity

costs recipient:

costs sender:

costs recipient: 10 ¢ per spam

costs sender: < 0.001 ¢ per spam

10 million Viagra spams → 1 sale

$3.5 million in revenue per year, for one botnet

why is this possible?

why is this possible?

bots

cost of spam not born by those enabling it

(an externality)

solution?

- regulation: prohibit the harmful activity
- taxation: tax the harmful activity, so market price reflects the true cost to society
- liability: make those causing harm liable for end effects
- mitigation: develop solutions so others are harmed less

Firm Is Accused of Sending Spam, and Fight Jams Internet

By JOHN MARKOFF and NICOLE PERLROTH

A squabble between a group fighting spam and a Dutch company that hosts Web sites said to be sending spam has escalated into one of the largest computer attacks on the Internet, causing widespread congestion and jamming crucial infrastructure around the world.

Millions of ordinary Internet users have experienced delays in services or could not reach a particular Web site for a short time.

However, for the Internet engineers who run the global network the problem is more worrisome. The attacks are becoming increasingly powerful, and computer security experts worry that if they continue to escalate people may not be able to reach basic Internet services, like e-mail and online banking.

let’s count the externalities:

let's count the externalities:

1. attackers used bots to send lots of traffic

let's count the externalities:

1. attackers used bots to send lots of traffic
2. attackers exploited open DNS relays to boost amount of traffic

let's count the externalities:

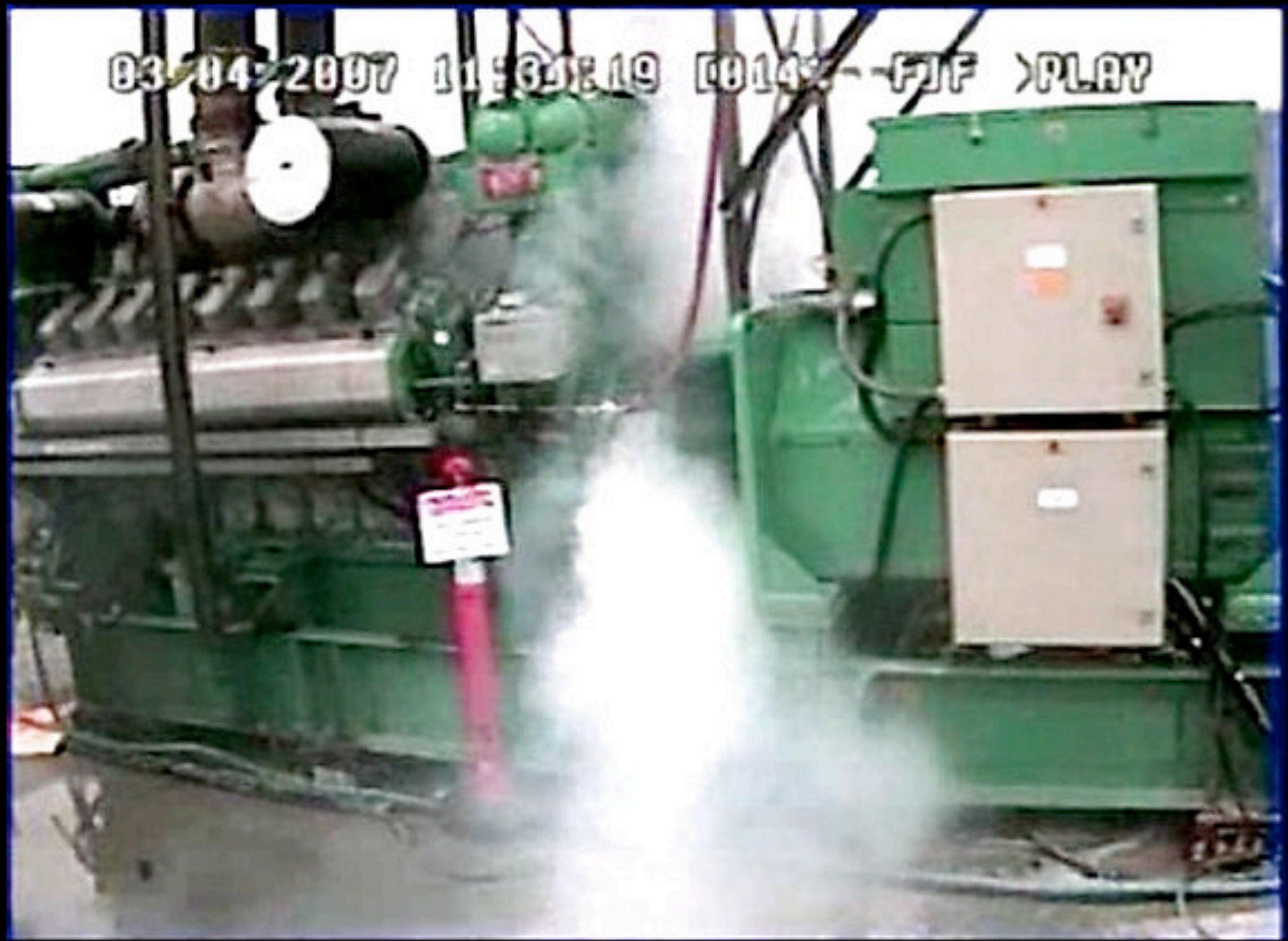
1. attackers used bots to send lots of traffic
2. attackers exploited open DNS relays to boost amount of traffic
3. ISPs don't block outgoing traffic with obviously spoofed source address

externalities make risks harder to manage

cyberwar

cyberespionage

cybercrime


03/04/2007 11:31:19 [014:--FJF >PLAY

Google has decided to stop censoring search results in China, after discovering that someone based in that country had attempted to hack into the e-mail accounts of human rights activists. The company disclosed the move in a startling announcement posted to its blog late Tuesday.

Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

Enlarge Photo

THIS STORY

» Google attack part of vast campaign
- Google hands China an Internet dilemma
- Statement from Google: A new approach to China

View All Items in This Story

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail

What Google might miss out on

Google said it may exit China,

Hackers in China Attacked The Times for Last 4 Months

By NICOLE PERLROTH

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and computer security experts have expelled the attackers and kept them from breaking back in.

The timing of the attacks coincided with the reporting for a Times investigation, published online on Oct. 25, that found that the relatives of Wen Jiabao, China's prime minister, had accumulated a fortune worth several billion dollars through business dealings.

Washington Post Joins List of News Media Hacked by the Chinese

By NICOLE PERLROTH

SAN FRANCISCO — The question is no longer who has been hacked. It's who hasn't?

The Washington Post can be added to the growing list of American news organizations whose computers have been penetrated by Chinese hackers.

After The New York Times reported on Wednesday that its computers as well as those of Bloomberg News had been attacked by Chinese hackers, The Wall Street Journal said on Thursday that it too had been a victim of Chinese cyberattacks.

CONVERT INSTALLS TO CASH WITH HIGH RATES

GoldInstall

Main | Sign up | Login | Rates | Contacts | **Terms of service** | FAQ

Prices

Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$
DK	20$
ES	30$
AU	55$
FR	30$
NL	20$
NO	20$
PT	30$
LB	6$

PayPal

Please fill in the correct information for the following category to verify your identity.

Security Measures

Email address:

PayPal Password:

Full Name:

SSN: - -

Card Type: Card Type

Card Number:

Expiration Date: Month / Year (mm/yyyy)

Card Verification Number (CVV2):

Street:

City:

Country: United States

Zip Code:

Telephone:

Verified By Visa / Mastercard Securecode:

Date of Birth: - - (Ex: dd-mm-yyyy)

Submit Form

By clicking the button "Submit Form" you confirm your identity with us. The form is submitted instantly.

Your session will be closed after you verify your information.

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should **never** give your PayPal password to anyone, including PayPal employees.

eBay sent this message from (pajv21).
Your registered name is included to show this message originated from eBay. Learn more.

Message from eBay member , pajv21

Do not respond to the sender if this message requests that you complete the transaction outside of eBay. This type of offer is against eBay policy, may be fraudulent, and is not covered by buyer protection programs. Learn More.

I can do for $385.00 with shipping. Waiting for your answer asap.

Thank you.

Did this answer your question? If not, let the seller know.

Respond

View Item: http;//cgi.ebay.com/ws/eBayISAPI.dll? ViewItem&item=130312669787

Item Id: 130312669787
End time: Mar 03, 2011 09:38:06 PDT
Buyer: pajv21 (381)
Feedback:**100 % Positive**
Member: since 26-May-06
Location: United States
Listing Status: This message was sent while the listing was **active.**

Marketplace Safety Tip

- Keep your money safe - never pay for items with cash or instant money transfer services, such as Western Union or MoneyGram. In the past some sellers have exploited these payment methods in order to defraud buyers, so eBay has banned them from the site.

Done

Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/

Go Links

ebay

eBay Buyer Protection Learn more NEW

Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- **Bid, buy and find bargains** from all over the world
- **Shop with confidence** with PayPal Buyer Protection
- **Connect with the eBay community** and more!

Register

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID

I forgot my user ID

Password

I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not

Thursday, April 4, 13

VNC: throwaway-xp-026

Recycle Bin

Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/

Go Links

eBay Buyer Protection Learn more NEW

Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- **Bid, buy and find bargains** from all over the world
- **Shop with confidence** with PayPal Buyer Protection
- **Connect with the eBay community** and more!

Register

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID jbieber

I forgot my user ID

Password ••••••••••••

I forgot my password

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not

start

Thursday, April 4, 13

VNC: throwaway-xp-026

Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php

Go Links

ebay

Please confirm your identity jbieber

Please answer security question below.

What is your mother's maiden name?

Smith

Answer the secret question you provided.

What is your other eBay user ID or another's member in your household?

NA

What email used to be associated with this account?

bieberlicious@hotmail.com

Have you ever sold something on eBay?

start eBay sent this messa Identity Confirmation 8:40 PM

Thursday, April 4, 13

VNC: throwaway-xp-026

Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/fin.php

Go Links

Buy Sell My eBay Communit

Bucks You're Invited! Join eBay Bucks.

All Categories Search Advanced Search

Categories Motors Stores Daily Deal

eBay Se Resolutio

Thanks jbieber. Your identity has been confirmed.

Now you can pick up where you left off.

Save Profile

About eBay | Announcements | Security Center | Resolution Center | eBay Toolbar | Policies | Government Relations | Site Map | Help

eBay Buyer Protection We'll cover your purchase price plus original shipping. Learn more

Copyright © 1995-2010 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

eBay official time

VeriSign Identity Protection

start

Thursday, April 4, 13

VNC: throwaway-xp-026

Recycle Bin

http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&Item=350121605127&Category=147218&_trkparms=algo= - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&Item=350121605127&Category=147218&_trkparms=algo%3DLVI%26its%3DI%26otn%3D1

Go Links

Go My eBay | Sell | Community | Customer Support

Welcome! Sign in or register.

CATEGORIES | FASHION | MOTORS | DEALS | CLASSIFIEDS

eBay Buyer Protection Learn more

This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.

About eBay | Security Center | Buyer Tools | Policies | Stores | Site Map | eBay official time

Copyright © 1995-2011 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

start

cyberwar

cyberespionage

cybercrime

cyberwar

cyberespionage

cybercrime

exercise: name some externalities

general strategies for dealing with risk:

- prevention: reduce probability of bad thing
- mitigation: reduce cost of bad thing
- risk transfer: shift cost to someone else (insurance, taxation, liability, ...)