

Impersonation

CS 161: Computer Security

Prof. Vern Paxson

**TAs: Devdatta Akhawe, Mobin Javed
& Matthias Vallentin**

<http://inst.eecs.berkeley.edu/~cs161/>

March 1, 2011

Announcements

- Midterm next Tuesday March 8th
 - Scope is course material up through today
 - You can bring a *single sheet* of notes
 - Two-sided, viewable w/o assistance
 - (FYI: you might want to keep this for the final)
- My office hours the week of March 7th will be by appointment
- **Guest lecture** this Thursday (March 3rd), Prof. David Wagner
- Reminder, HW #2 due **5PM** on Friday

Goals For Today

- A broad look at the problem of *impersonation*: threats based on something not being what it appears to be
- Web attacks: misleading users regarding their clicks
- Phishing: misleading users regarding with whom they are interacting
- CAPTCHAs: telling humans apart from “bots”
- Analyzing email headers for legitimacy (time permitting)

Attacks on User *Volition*

- Browser assumes clicks & keystrokes = *clear indication of what the user wants to do*
 - Constitutes part of the user's *trusted path*
- Attack #1: commandeer the focus of user-input
- Attack #2: mislead the user regarding true focus (“**click-jacking**”)

Click-Jacking

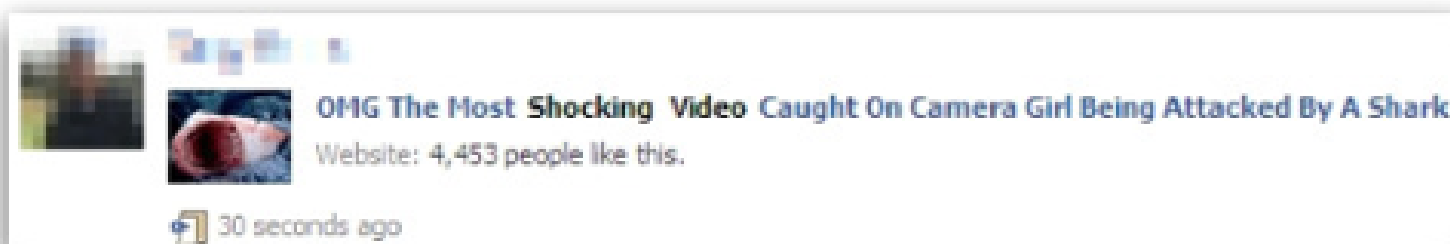
- Demo #1: you think you're typing to a familiar app, but you're not (demo)

Click-Jacking

- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are (demo)



OMG The Most Shocking Video Caught On Camera Girl Being Attacked By A Shark





Your account |  | Contact | United States (Change)

Solutions Products Support Communities Company Downloads Store

Home / Support / Documentation / Flash Player Documentation /

Flash Player Help

Global Security Settings panel

TABLE OF CONTENTS

Flash Player Help

Settings Manager

- Global Privacy Settings Panel
- Global Storage Settings Panel
- Global Security Settings Panel
- Global Notifications Settings Panel
- Website Privacy Settings Panel
- Website Storage Settings Panel

Display Settings

Local Storage Settings

Microphone Settings



Let's click here!

Click-Jacking

- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are
 - You might click on what the attacker wants
no matter where you click! (demo)

Click-Jacking

- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are
- Demo #3: you definitely meant to click somewhere else

Adblock Plus :: Add-ons for Firefox

◀ ▶ ↺ ✕ 🏠

Mozilla Corporation (US) https://addons.mozilla.org/en-US/firefox/addon/1865 ☆ Google 🔍

Most Visited ▾ Getting Started Latest Headlines 📡 NY Times Google News Daily ▾ Weather 294 United Traffic Papers US9 IMC CSET >>

🦊 Adblock Plus :: Add-ons for Firefox +

🛒

mozilla


Register or Log in Other Applications ▾

Add-ons for Firefox

🔍 search for add-ons within all add-ons ▶

Advanced ▾

Add-ons for Firefox

 **Adblock Plus 1.1.3**
by [Wladimir Palant](#)

📄 e news, l
copy Boo
Set As Desktop Background
Properties
Adblock Image...
State: MD ▾

Share this Add-on

Ever been annoyed by all those ads and banners on the internet that often take longer to download than everything else on the page? Install Adblock Plus now and get rid of them.

For a quick overview watch <http://www.youtube.com/watch?v=oNvb2SjVjil>

+ Add to Firefox

recommended

Version 1.1.3

See All Privacy & Security Add-ons ▶

Other add-ons by [Wladimir Palant](#)
Adblock Plus ▾

Need help with this add-on?
▪ [Visit the support site](#)

Done



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



Adblock Plus *(Wladimir Palant)*

<https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon>

Cancel

Install (5)



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



Addblock Plus *(Wladimir Palant)*

<https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon>

Cancel

Install (4)



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



Addblock Plus *(Wladimir Palant)*

<https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon>

Cancel

Install (3)



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



Adblock Plus *(Wladimir Palant)*

<https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon>

Cancel

Install (2)



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



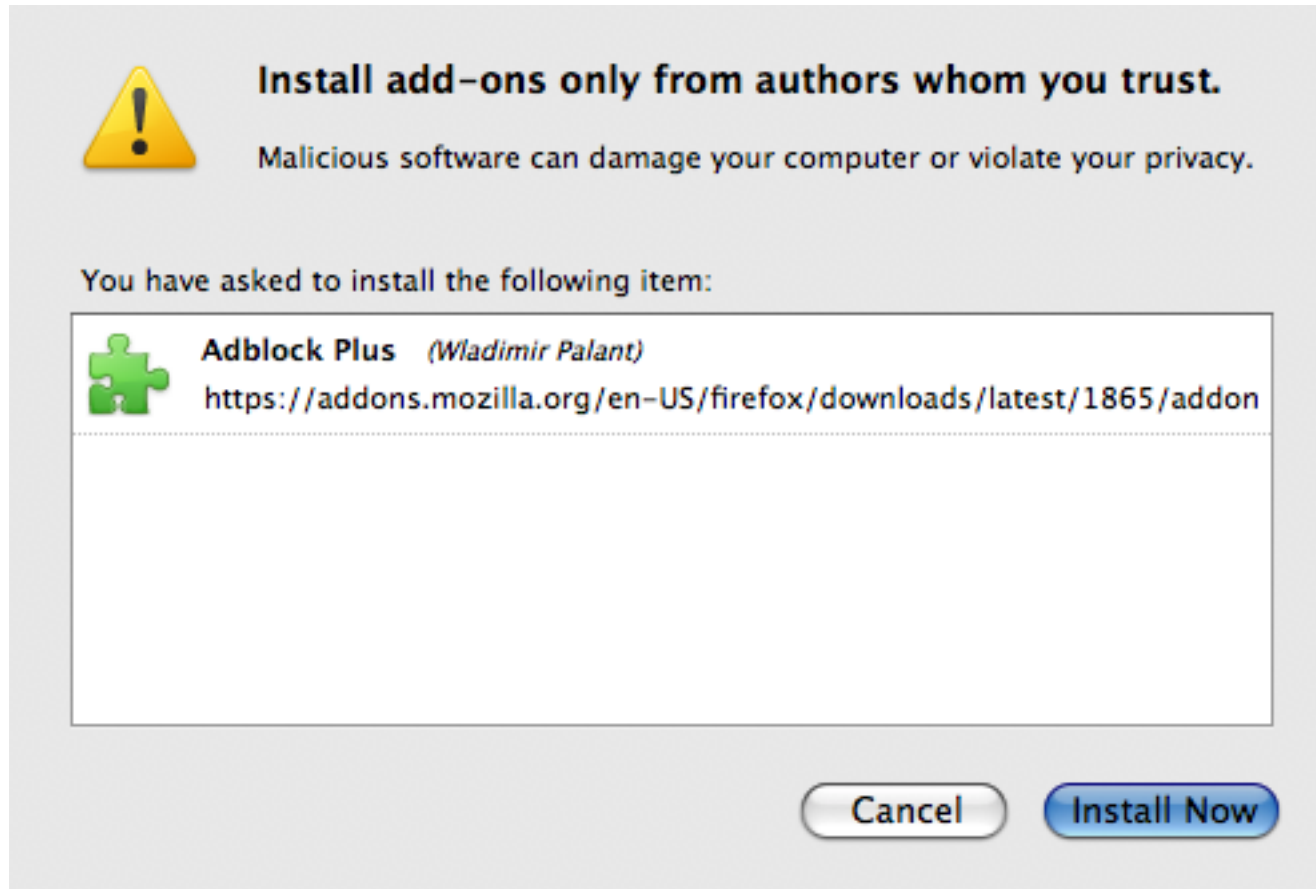
Addblock Plus *(Wladimir Palant)*

<https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon>

Cancel

Install (1)

Why Does Firefox Make You Wait?



... to keep you from being tricked into clicking!

Defending Against Clickjacking

- Main defense: *frame busting*
- Web site ensures that its “vulnerable” pages can’t be included as a **frame** inside another browser frame



Attacker implements this by placing Twitter's page in a "Frame" inside their own page. Otherwise they wouldn't overlap.

Defending Against Clickjacking

- Main defense: *frame busting*
- Web site ensures that its “vulnerable” pages can’t be included as a **frame** inside another browser frame
 - So user can’t be looking at it with something invisible overlaid on top ...
 - ... nor have the site invisible above something else
- Conceptually implemented with Javascript like:

```
if (top.location != self.location)
    top.location = self.location;
```
- (Note: actually quite tricky to get this right!)

Related UI Sneakiness

- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are
- Demo #3: you definitely meant to click somewhere else
- Demo #4: you've got a lot on your mind (demo)

Related UI Sneakiness

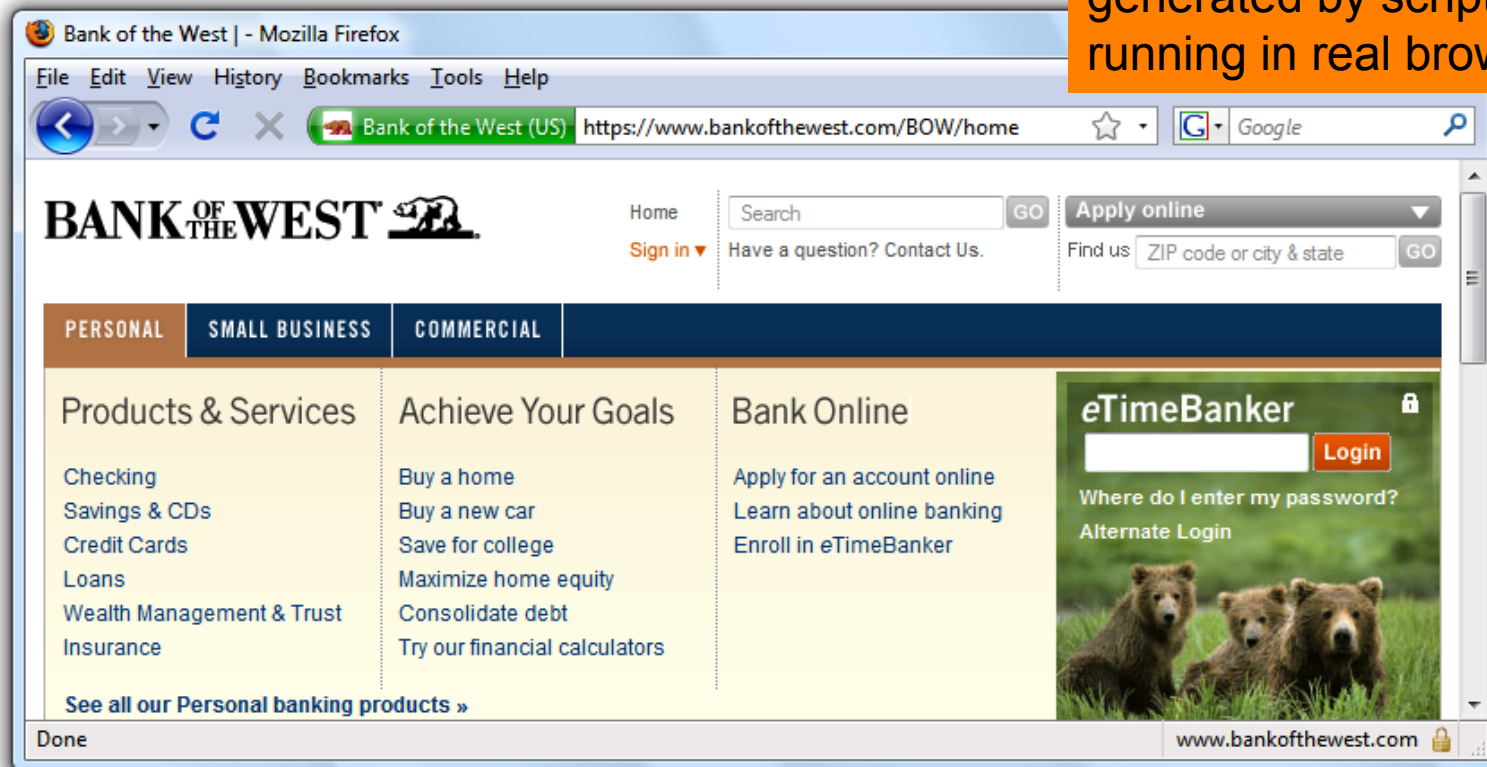
- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are
- Demo #3: you definitely meant to click somewhere else
- Demo #4: you've got a lot on your mind (demo)
 - *Tabnabbing*

Related UI Sneakiness

- Demo #1: you think you're typing to a familiar app, but you're not
- Demo #2: you don't think you're typing to a familiar app, but you are
- Demo #3: you definitely meant to click somewhere else
- Demo #4: you've got a lot on your mind (demo)
 - *Tabnabbing*
- Demo #5: you're living in *The Matrix*

“Browser in Browser”

*Apparent browser is just a **fully interactive image** generated by script running in real browser!*



5 Minute Break

Questions Before We Proceed?

Phishing



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

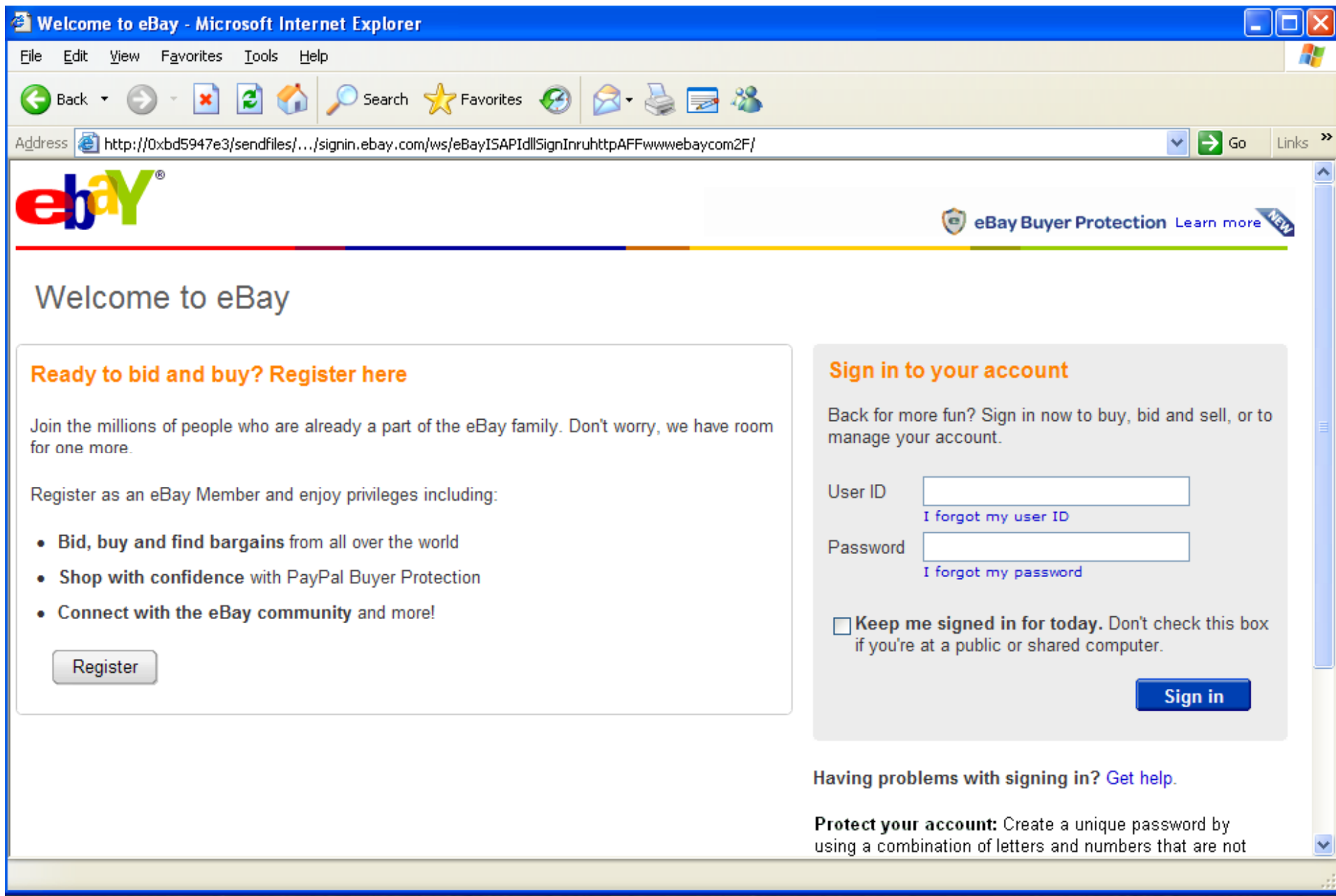
Listing Status: This message was sent while the listing was **active**.



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.



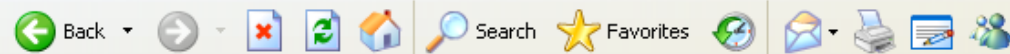




Recycle Bin

Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help



Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPI.dll?SignInruhttpAFFwww.ebay.com2F/

Go

Links

eBay Buyer Protection [Learn more](#)

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](#)

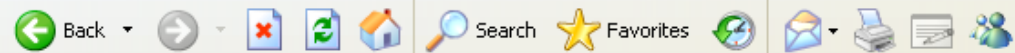
Having problems with signing in? [Get help.](#)

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



Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help



Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPI.dll?SignInhttpAFFwww.ebay.com2F/sQuestion.php

Go

Links



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

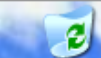
Have you ever sold something on eBay?



eBay sent this messa...

Identity Confirmation...

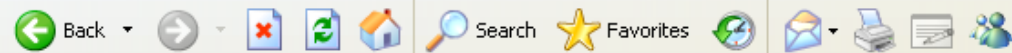
8:40 PM



Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help



Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPI.dll?SignInruhttpAFFwww.ebay.com2F/fin.php

Go

Links >>

**Bucks** You're Invited! Join **eBay Bucks**.[Buy](#) [Sell](#) [My eBay](#) [Communi](#) All Categories [Advanced Search](#)[Categories](#) [Motors](#) [Stores](#) [Daily Deal](#)[eBay Seller Resolution](#)**Thanks jbieber. Your identity has been confirmed.**

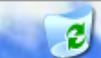
Now you can pick up where you left off.

[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](#)

eBay sent this messa...

Identity Confirmation...

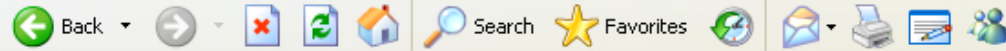
8:41 PM



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



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

Go

Links

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](#).



eBay sent this messa...

http://cgi.ebay.com/...

8:41 PM

The Problem of Phishing

- Arises due to mismatch between reality & user's:
 - Perception of how to **assess legitimacy**
 - Mental model of what attackers can control
 - Both Email and Web
- Coupled with:
 - Deficiencies in how web sites authenticate
 - In particular, “replayable” authentication that is vulnerable to theft
- How can we tell when we're being phished?



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.





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**.

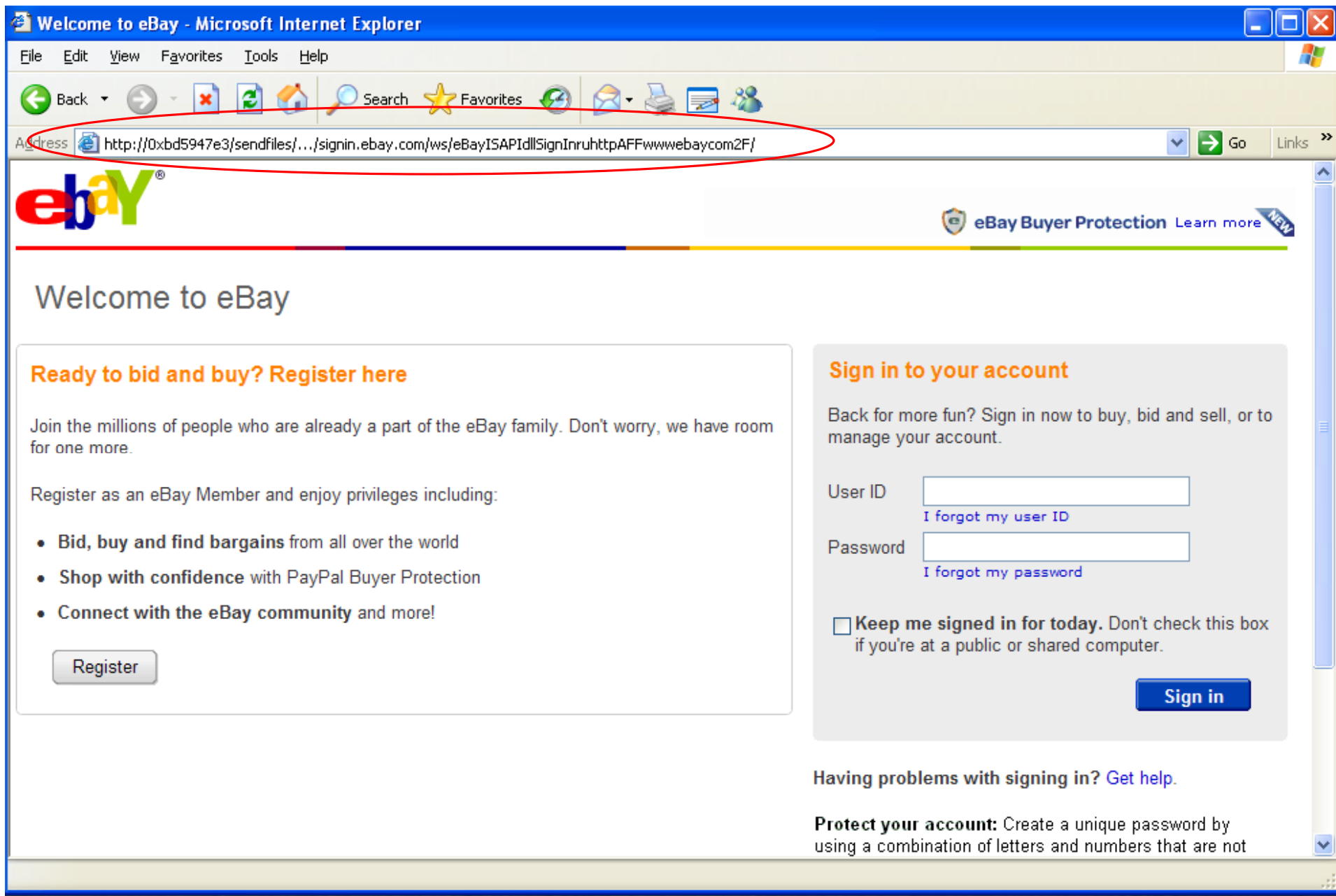


Marketplace Safety Tip

- 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.

Check the URL before clicking?

```
<a href="http://www.ebay.com/"  
  onclick="location='http://hackrz.com/'">
```



Address  <http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPI.dll?SignIn&httpAFFwww.ebay.com2F/>

Exploits a misfeature in IE that interprets
a number here as a 32-bit IP address

0xbd5947e3 = 189.89.71.227

```
dig -x 189.89.71.227
```

```
; <<>> DiG 9.6.0-APPLE-P2 <<>> -x 189.89.71.227
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24037
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;227.71.89.189.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
227.71.89.189.in-addr.arpa. 86400 IN      PTR
                           227.71.89.189.cliente.interjato.com.br.

;; AUTHORITY SECTION:
71.89.189.in-addr.arpa. 86399 IN      NS      ns2.interjato.com.br.
71.89.189.in-addr.arpa. 86399 IN      NS      ns1.interjato.com.br.

;; Query time: 511 msec
;; SERVER: 128.32.153.21#53(128.32.153.21)
;; WHEN: Tue Mar  1 17:37:52 2011
;; MSG SIZE  rcvd: 132
```


whois 189.89.71.227

The following results may also be obtained via:

<http://whois.arin.net/rest/nets;q=189.89.71.227?showDetails=true&showA>
e
#

NetRange: 189.0.0.0 - 189.255.255.255

CIDR: 189.0.0.0/8

OriginAS:

NetName: NET189

NetHandle: NET-189-0-0-0-1

Parent:

NetType: Allocated to LACNIC

...

...

inetnum: 189.89.64/20

aut-num: AS28184

abuse-c: EMR5

owner: TECHNET NETWORKING LTDA

ownerid: 000.872.797/0001-17

responsible: Erich matos Rodrigues

country: BR

Check the URL in address bar?



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

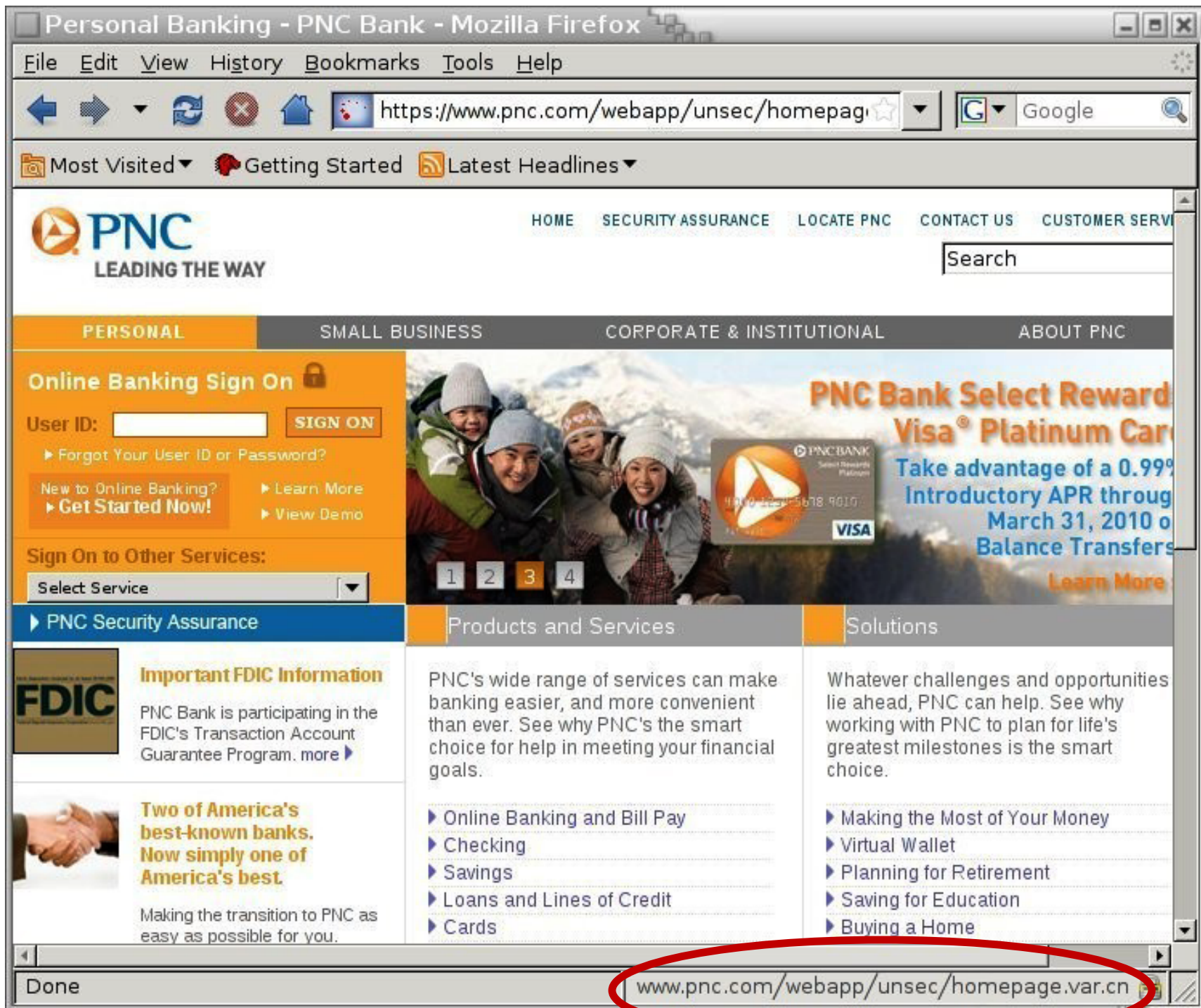
[I forgot my password](#)

☐ **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: Check that the Web address in your browser starts with <https://signin.ebay.com/>. [More account security tips.](#)



Homograph Attacks

- International domain names can use international character set
 - E.g., Chinese contains characters that look like / . ? =
- **Attack:** Legitimately register var.cn ...
- ... buy legitimate set of HTTPS certificates for it ...
- ... and then create a subdomain:
`www.pnc.com/webapp/unsec/homepage.var.cn`

Check for padlock?



WACHOVIA



LOGIN



User ID:

☐

Remember my User ID

Password:

(case sensitive)

Service:

Choose a service... ▾

Login

Forgot [User ID](#) or [Password](#)?

Retirement Plan Participants: [Login](#)

Education Loan Customers: [Login](#)

PERSONAL FINANCE

[Online Services](#)

Online Banking with BillPay

Mobile Banking

Online Brokerage

More...

[Retirement Planning](#)

Tools & information for
Lifetime Retirement Planning

[Investing](#)

Accounts & Services

IRAs

More...

[Banking](#)

Checking

Savings & CDs

Credit Cards

Check Cards

More...

[Lending](#)

Mortgage

Home Equity **New!**

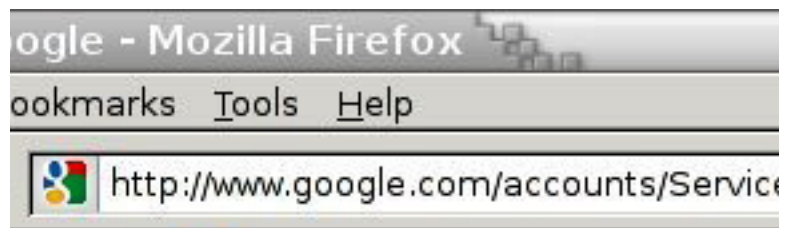
Education Loans

Vehicle Loans

[Rates](#)

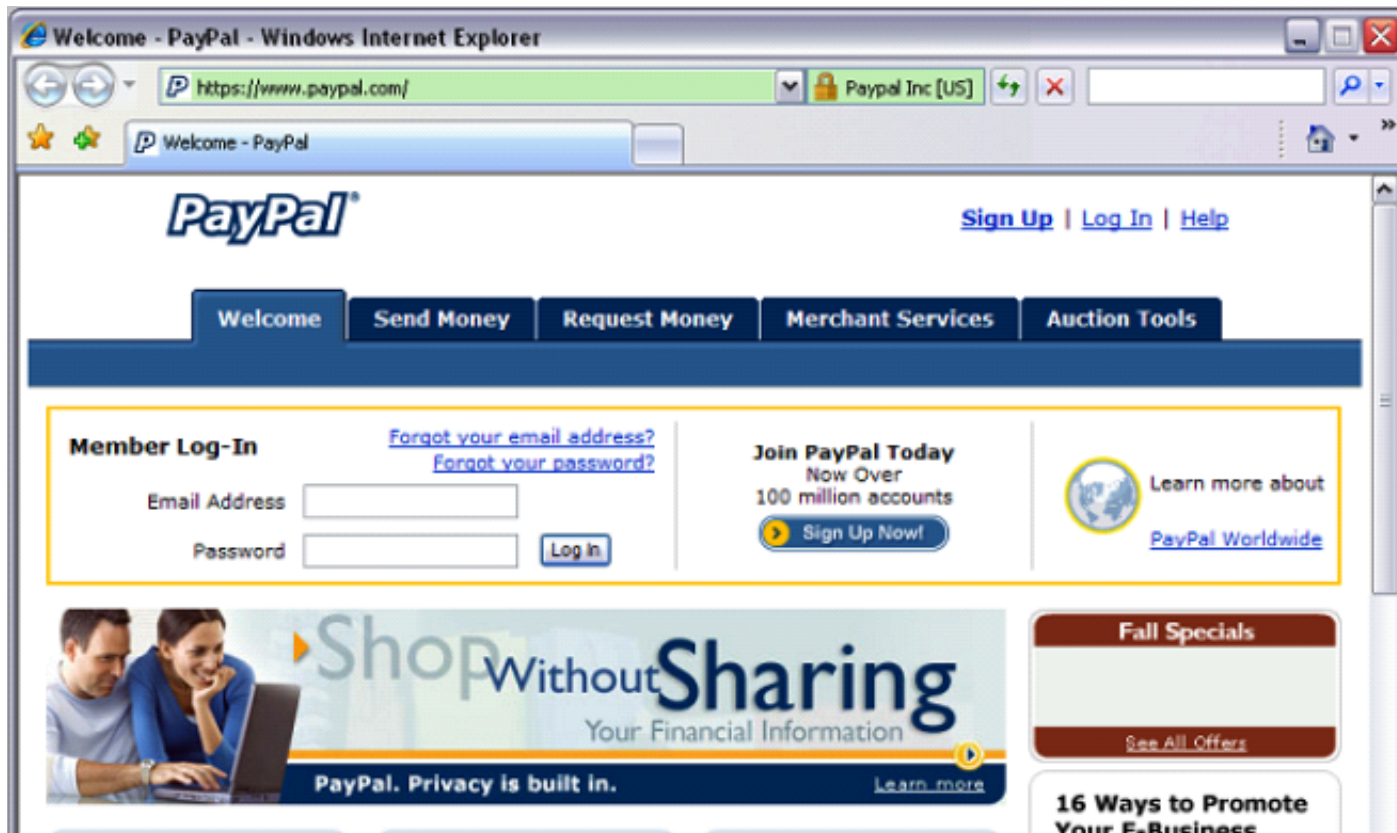
Mortgage Rates

▶ [English](#)

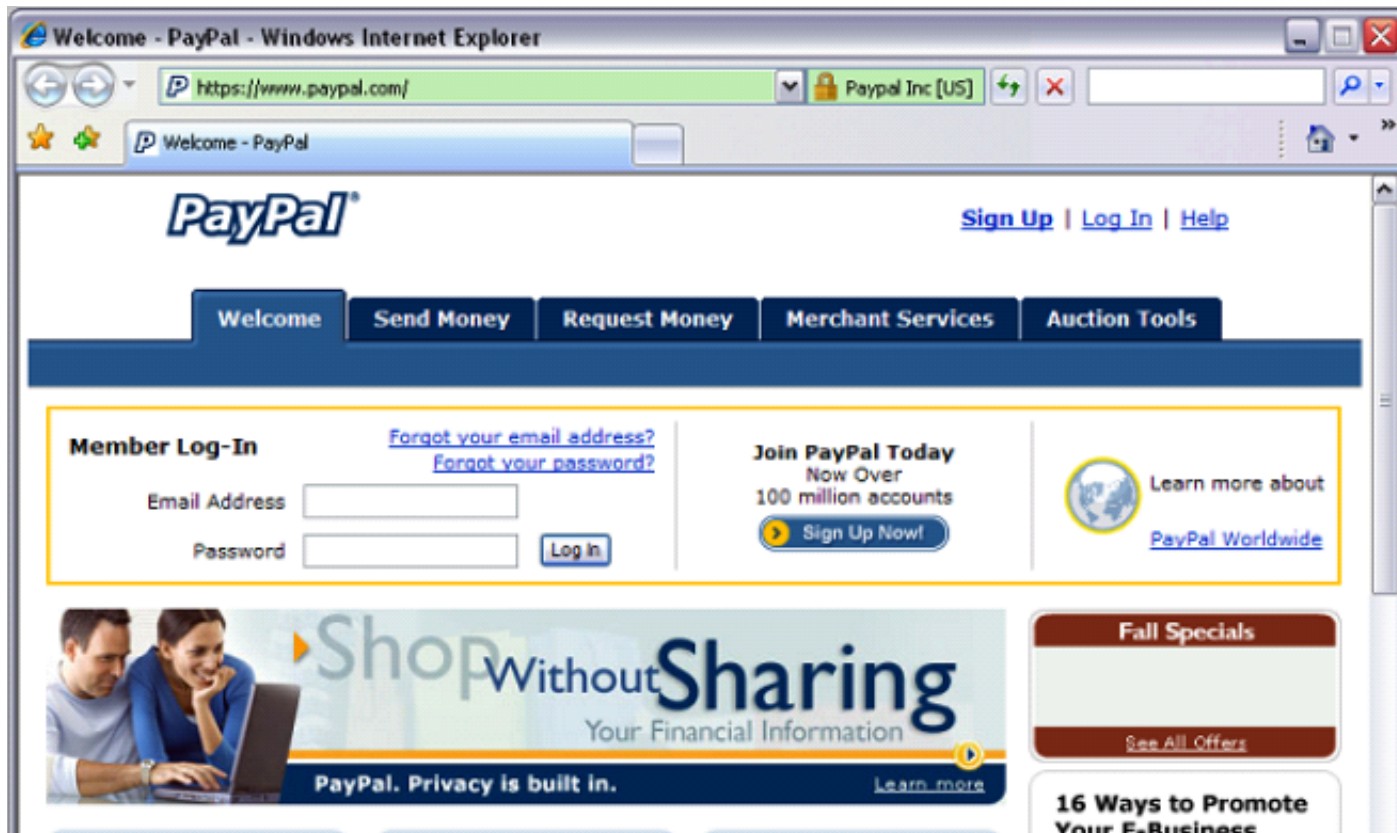


Add a clever .favicon with a picture of a padlock

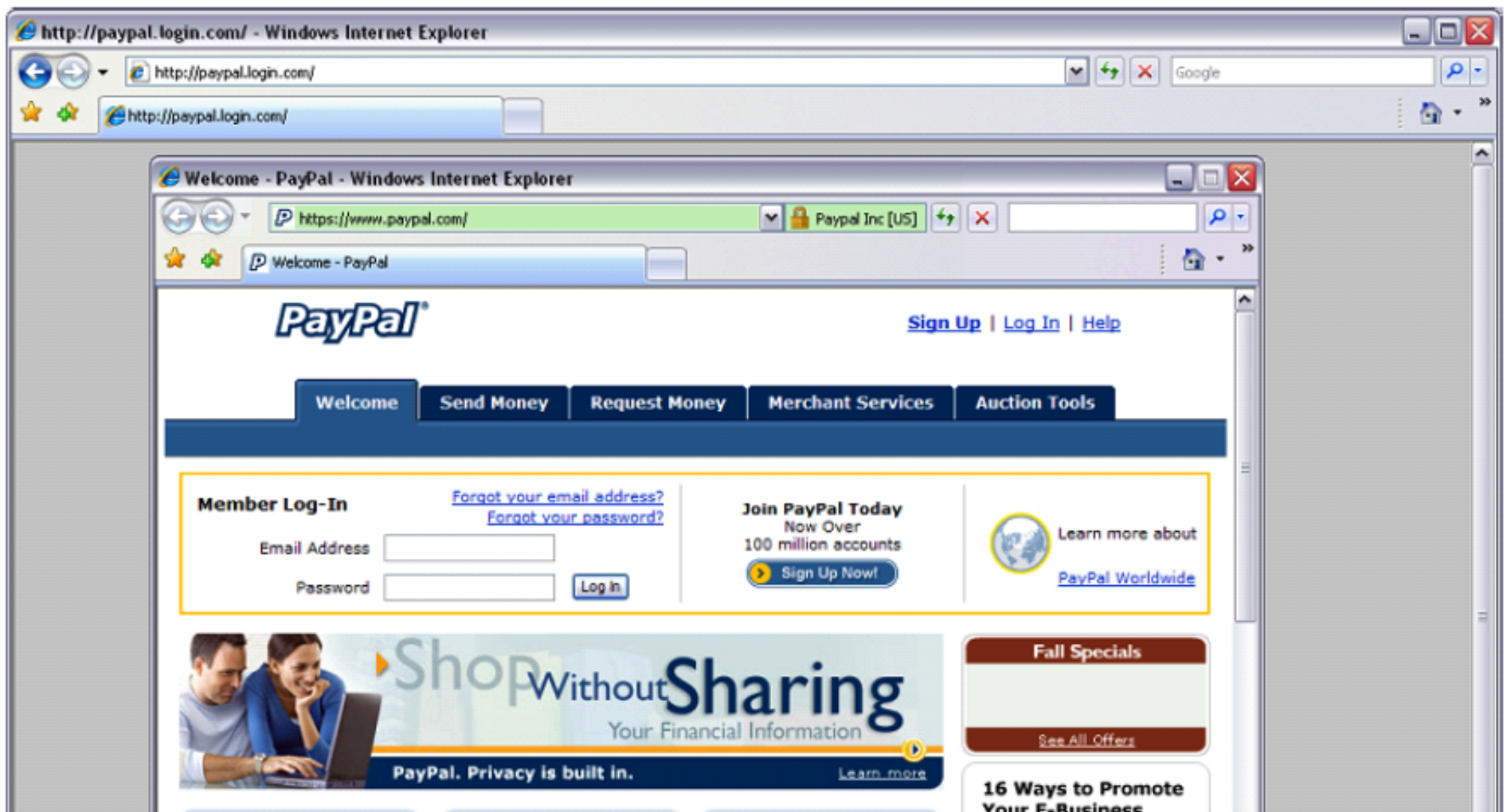
Check for “green glow” in address bar?



Check for everything?



“Browser in Browser”



“Spear Phishing”

From: Lab.senior.manager@gmail.com
Subject: FW: Agenda
Body: This below agenda just came in form from Susan, please look at it.
>From: Norris, Susan (ORO)
>To: Manager, Senior; Rabovsky, Joel MJ
>Subject: Agenda
>Thanks, nice to know that you all care this so much!
>
>Susan Norris
>norrissg@oro.doe.gov
Attached: Agenda Mar 4.pdf

Targeted phishing that includes details
that seemingly must mean it's legitimate

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or IntelLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

<http://mv.net.md/update/update.zip>

or

<http://www.sendspace.com/file/xwc1pi>

Yep, this is itself a
spear-phishing attack!

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us

Sophisticated phishing

- Context-aware phishing – 10% users fooled
 - Spoofed email includes info related to a recent eBay transaction/listing/purchase
- Social phishing – 70% users fooled
 - Send spoofed email appearing to be from one of the victim's friends (inferred using social networks)
- West Point experiment
 - Cadets received a spoofed email near end of semester: *“There was a problem with your last grade report; click here to resolve it.”* 80% clicked.


CAPTCHAs

Visual code | [Audio code](#)

[Help](#)



Type the code shown

 [Try a new code](#)

By clicking the "Create My Account" button below, I certify that I have read and agree to the [Yahoo! Terms of Service](#), [Yahoo! Privacy Policy](#) and [Communication Terms of Service](#), and to receive account related communications from Yahoo! electronically. Yahoo! [automatically identifies](#) items such as words, links, people, and subjects from your Yahoo! communications services to deliver product features and relevant advertising.

Create My Account

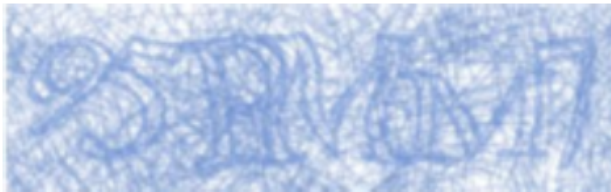
CAPTCHAs

- *Reverse Turing Test*: present “user” a challenge that’s easy for a human to solve, hard for a program to solve
- One common approach: distorted text that’s difficult for character-recognition algorithms to decipher

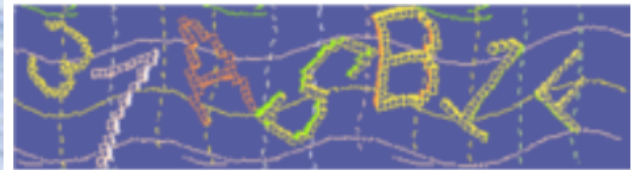




(a) Aol.



(b) mail.ru



(c) phpBB 3.0



(d) Simple Machines Forum



(e) Yahoo!



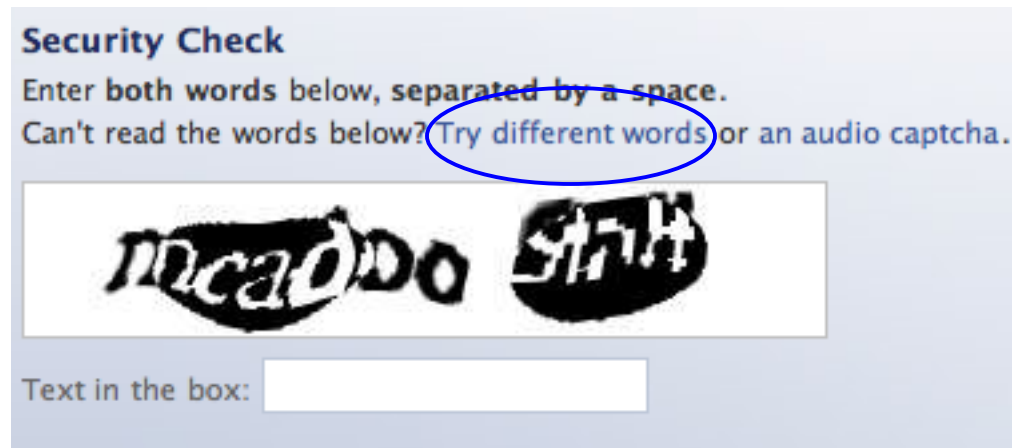
(f) youku

Figure 1: Examples of CAPTCHAs from various Internet properties.

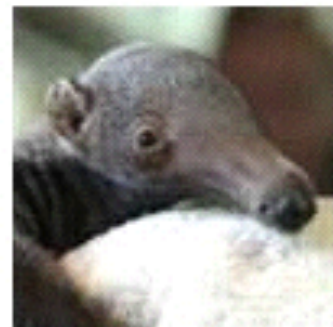
Problems?

Issues with CAPTCHAs

- Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans



Click 3 pictures of kittens to submit



The KittenAuth system. Source: ThePCSpy.com.

Issues with CAPTCHAs

- Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans



- *Accessibility*: not all humans can see!
- *Granularity*: not all bots are bad! (e.g., crawlers)

Issues with CAPTCHAs, con't

- If generating a CAPTCHA is somewhat expensive, *the mechanism itself is a DoS vulnerability*



reddit

hot

new

browse

stats



Clicking this link loads 120,000 copies of the RIAA's captcha. Clicking would be wrong, don't do it. (antisocial.propagation.net)

452 points posted 4 days ago by mridlen 292 comments

Issues with CAPTCHAs, con't

- If generating a CAPTCHA is somewhat expensive, *the mechanism itself is a DoS vulnerability*
- Final problem: CAPTCHAs are inherently vulnerable to *outsourcing* attacks
 - Attacker gets real humans to solve them

Google

http://www.google.com/

NY Times Google News Daily Weather 294 United Traffic Papers HN09 IMC Google Maps RSS (1) Movies BART Wikis Calories Blog

Google

Web Images Videos Maps News Shopping Gmail more

iGoogle | Search settings | Sign in



"crack captcha"

crack captcha php

Google Search

I'm Feeling Lucky

[Advanced Search](#)
[Language Tools](#)

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2009 - [Privacy](#)

Browser window: "crack captcha" - Google Search

Address bar: <http://www.google.com/search?hl=en&source=hp&q=%22crack+captcha%22&aq=f&oq=&aqi=g1>

Search bar: "crack captcha" Search [Advanced Search](#)

Web [Images](#) [Videos](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more](#) [Search settings](#)

Web [+ Show options...](#) Results 1 - 10 of about 17,700 for "crack captcha". (0.17 seconds)

Captcha solving www.decaptcher.com Cheap captcha solving Cheap programs for advertisement Sponsored Link

Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business efficiency now!

Follow these steps:

- Register
- Login and follow the link inside to load funds to your account.
- Your request will be processed ASAP.

You pay for correctly recognized CAPTCHAs only

The price is \$2 for 1000 CAPTCHAs. We accept payments from \$10.

If you use a third-party software the price could be different, contact the software vendor for more information.

Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?

We have no restrictions about IP: with DeCaptcher you can bypass CAPTCHA from as many IPs as you need.

Hi. I need to crack captcha. Do you provide a captcha decoders?

DeCaptcher CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones

Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá dalawá tatlo	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um dois três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один два три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று இரண்டு மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een twee drie	4.09	1.36	0.00	0.00	1.22	31.1	6.30
Hindi	एक दो तीन	10.5	5.38	2.47	1.52	6.30	9.49	5.94
German	eins zwei drei	3.62	0.72	0.00	1.46	0.58	29.1	5.91
Malay	satu dua tiga	0.00	1.42	0.00	0.00	0.55	29.4	5.23
Vietnamese	một hai ba	0.46	2.07	0.00	0.00	1.74	18.1	3.72
Korean	일 이 삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد اثنين ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক দুই তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು ಎರಡು ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	ᑭᑭᑭ	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک دو سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.

Analyzing Email Headers

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or Intelink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

<http://mv.net.md/update/update.zip>

or

<http://www.sendspace.com/file/xwc1pi>

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us

Delivery-Date: Wed Feb 10 10:51:55 2010

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]

by vpmmini.icipr.org with IMAP (fetchmail-6.3.11)

Received: "Headers" in the email message

for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -0800

Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135])

by ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895

for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST)

Authentication-Results: ee.lbl.gov; sender-id=softfail header.from=

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)

(envelope-from <w63697@uw03.uniweb.no>)

id 1NfHf9-0002n7-Md

for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100

To: vern@ee.lbl.gov

Subject: RE: Russian spear phishing attack against .mil and .gov emp

From: jeffrey@cia.gov

Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>

Date: Wed, 10 Feb 2010 19:51:47 +0100

X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov

X-Virus-Status: Clean

Content-Length: 1116

To/Subject/From/etc. are completely
under the attacker's control

To: vern@ee.lbl.gov

Subject: RE: Russian spear phishing attack against .mil and .gov em

From: jeffrey@cia.gov

Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>

Date: Wed, 10 Feb 2010 19:51:47 +0100

Any headers below them *may* also
be under the attacker's control

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffrey@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov
X-Virus-Status: Clean
Content-Length: 1116

This header tells us about the first delivery
“hop”. It’s supposedly reported by a
machine uw03.uniweb.no, but who knows ...

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
(envelope-from <w63697@uw03.uniweb.no>)
id 1NfHf9-0002n7-Md
for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffrey@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov
X-Virus-Status: Clean
Content-Length: 1116

However, headers for subsequent hops are *prepended*.

So we can start at the **top** of the headers, which came from our trusted mailer, and decide how much trustworthy information we can find ...

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)
(envelope-from <w63697@uw03.uniweb.no>)
id 1NfHf9-0002n7-Md
for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100
To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov em
From: jeffrey@cia.gov
Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>
Date: Wed, 10 Feb 2010 19:51:47 +0100
X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov
X-Virus-Status: Clean
Content-Length: 1116

Delivery-Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmi.ici.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:!

This header is my own system (vpmini.ici.org) stating that it retrieved the message from mailhost.icsi.berkeley.edu.

I trust vpmini.ici.org, and therefore I believe the previous hop really was mailhost.icsi.berkeley.edu.

Delivery-Date: Wed Feb 10 10:51:55 2010

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]

by vpmmini.icsi.org with IMAP (fetchmail-6.3.11)

for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:55

Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])

by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) with

for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -0800

mailhost.icsi.berkeley.edu is integrated with
fruitcake.icsi.berkeley.edu (that's why the name is
different in this header).

I trust the ICSI mailer, so I will trust this Received
header too. It tells me that the prior hop was ee.lbl.gov
(which I also trust).

Delivery-Date: Wed Feb 10 10:51:55 2010
Received: from mailhost.icsi.berkeley.edu [192.150.186.11]
by vpmmini.icir.org with IMAP (fetchmail-6.3.11)
for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:55 -0800
Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])
by fruitcake.ICSI.Berkeley.EDU (8.12.11.20060614/8.12.11) with ESMTP
for <vern@icsi.berkeley.edu>; Wed, 10 Feb 2010 10:51:50 -0800
Received: from uw03.uniweb.no (uw03.uniweb.no [91.207.158.135])
by ee.lbl.gov (8.14.4/8.14.4) with ESMTP id o1AIpmOf002895
for <vern@ee.lbl.gov>; Wed, 10 Feb 2010 10:51:48 -0800 (PST)

ee.lbl.gov reports that the message came from
uw03.uniweb.no.

I trust that information, but I do **not** trust that host.
So any information from that point below is
untrustworthy.

Delivery-Date: Wed Feb 10 10:51:55 2010

Received: from mailhost.icsi.berkeley.edu [192.150.186.11]

by vpmni.icir.org with IMAP (fetchmail-6.3.11)

for <vern@localhost> (single-drop); Wed, 10 Feb 2010 10:51:55

Received: from ee.lbl.gov (ee.lbl.gov [131.243.2.201])

R However, I have reliably learned that the message was
sent by a machine in Norway ... probably not where the
CIA has a mail server!

Authentication-Results: ee.lbl.gov; sender-id=softfail header.from=

Received: from w63697 by uw03.uniweb.no with local (Exim 4.66)

(envelope-from <w63697@uw03.uniweb.no>)

id 1NfHf9-0002n7-Md

for vern@ee.lbl.gov; Wed, 10 Feb 2010 19:51:47 +0100

To: vern@ee.lbl.gov

Subject: RE: Russian spear phishing attack against .mil and .gov emp

From: jeffrey@cia.gov

Message-Id: <E1NfHf9-0002n7-Md@uw03.uniweb.no>

Date: Wed, 10 Feb 2010 19:51:47 +0100

X-Virus-Scanned: clamav-milter 0.95.3 at ee.lbl.gov

X-Virus-Status: Clean

Content-Length: 1116