Human Factors
in
Computer Security

3/29/2010

Administrative Announcements

- Midterm 2 on Friday; in principle, everything up till & including Wednesday is fair game, but in practice we'll focus on material after MT1.
- Midterm 2 review tomorrow, Tuesday, 3/30, 6:30-8:30pm in 1 Pimentel.
- Joel's 10-11 section tomorrow (3/30) should go to 3105 Etcheverry (temporarily merged with Matt's section, just for tomorrow). Joel's 2-3 section meets at regular time and place.

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Security & Resolution center

Profile Update for mcorssen

Please place your credit or debit card on file. This assures us of your identity and keeps eBay a safe place to buy and sell. Your c
authorize us to do so to pay selling fees.

Credit or debit card
XXXX-XXXX-XXXX-2027 is Visa

Information is protected on eBay's secure servers.

Expiration date 08/09
--Month-- --Year--

Card identification number

3-digit number on the back of the card. For American Express, use the 4-digit number on the front. Learn more.

Pin code **Confirm pin**

Personal Identification Number (PIN) ensures that no one but you has access to your funds.

Registration address
Michael Corssen, 101 Blair Road, Oyste
Bay NY 11771, United States, 516 578-
7273

Mother's maiden name

Your date of birth
month day year

Social security number
nnn-nn-nnnn

Save Profile >

From: eBay **To:**
Subject: Congrats, Your PowerSeller Membership Has Been Upgraded

Your registered name is included to show this message originated from eBay. Learn more.

Dear eBay Member,

Congratulations! You've been on a super sales streak and it's time to recognize your achievements! Your membership has been upgraded to Gold.

Your business is a top priority at eBay and we're standing by to provide the support you need. That's where I come in. I'm Doug Derricott, your dedicated PowerSeller Gold Account Manager. As I learn more about your eBay business, I'm here to serve as a resource for your continued success.

To access your personalized PowerSeller portal page, just click the PowerSeller icon next to your User ID or vist www.ebay.com/powerseller and click "Member Sign In." It is your gateway to all the great benefits and services associated with your new status. Once you sign in, you can:

- See your monthly average sales, sold items, and PowerSeller level.
- Get updates on benefits and promotions, events, advanced selling strategies, and guidelines for using the eBay logo and icons.
- Download FREE PowerSeller business card and letterhead templates--print in color or black and white.
- Check requirements for the PowerSeller program and read answers to Frequently Asked Questions about the program and benefits.

Again, congratulations and best wishes for your continued success!

Regards,

Doug Derricott
Your Gold PowerSeller Account Manager

eBay sent this message to Michael Olsen (mhj7).
Your registered name is included to show this message originated from eBay. Learn more.

This member has a question for you.

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.

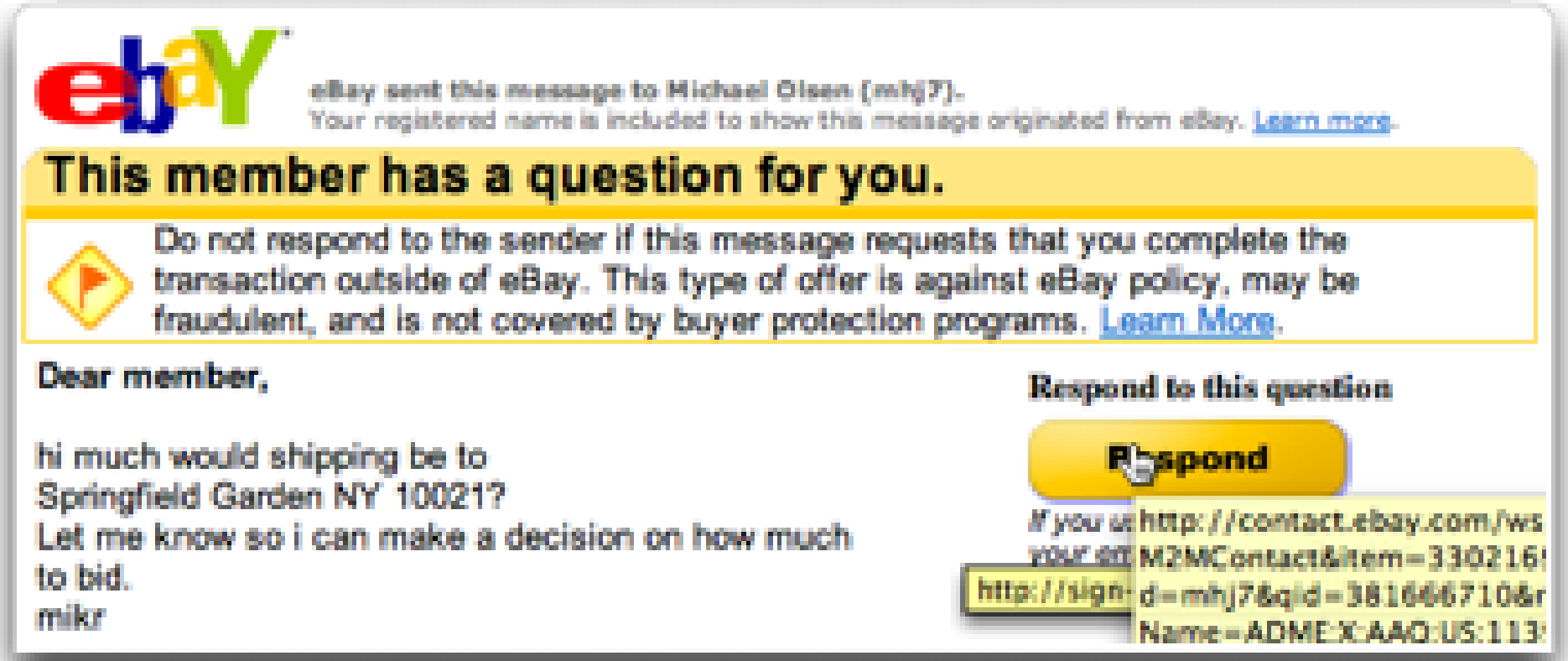
Dear member,

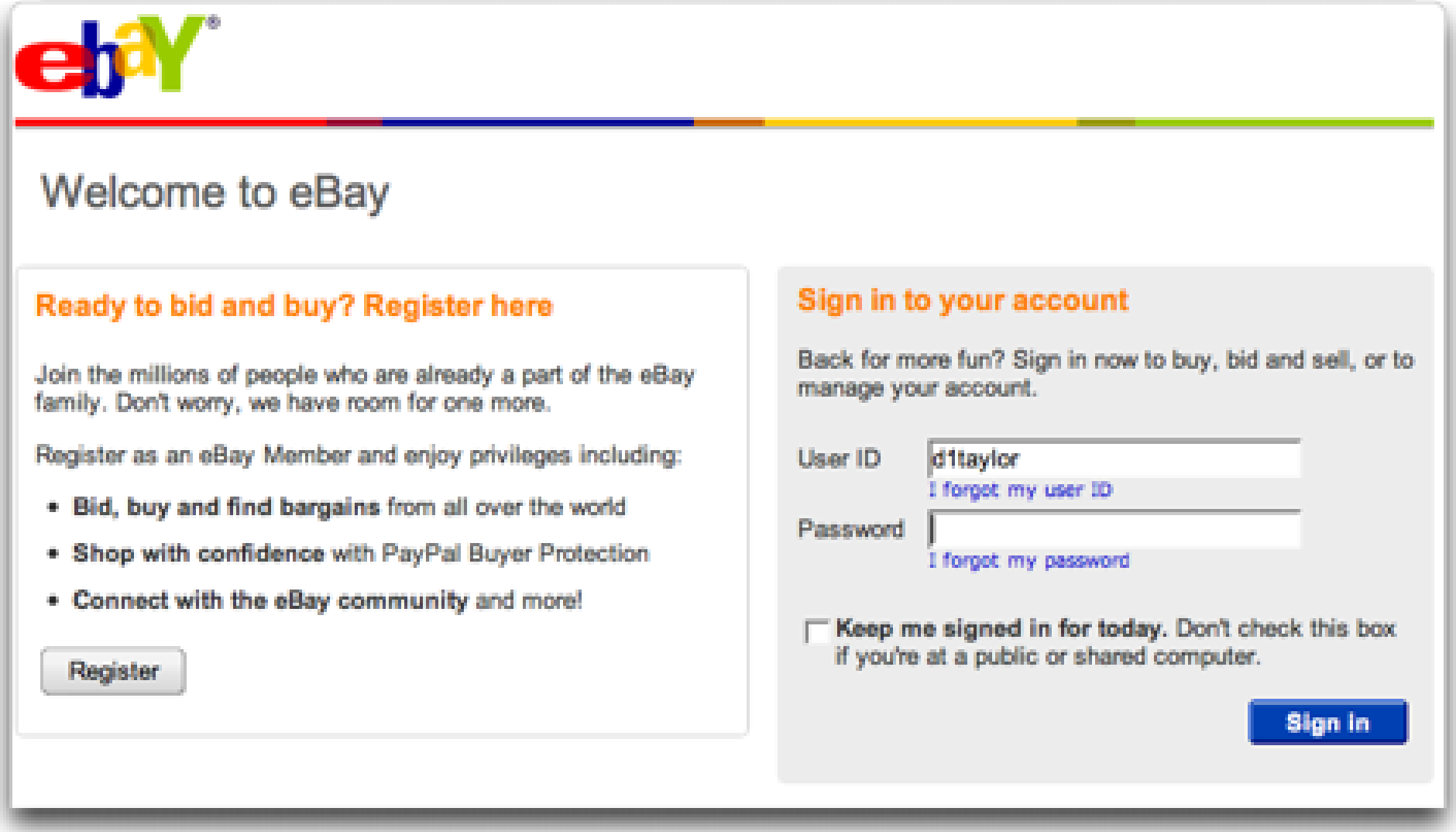
hi much would shipping be to
Springfield Garden NY 10021?
Let me know so i can make a decision on how much to bid.
mikr

Respond to this question

Respond

If you use My Messages to respond, your email address will not be shared


eBay sent this message to Michael Olsen (mhj7).
Your registered name is included to show this message originated from eBay. Learn more.
This member has a question for you.
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.
Dear member,
hi much would shipping be to
Springfield Garden NY 10021?
Let me know so i can make a decision on how much to bid.
mikr
Respond to this question
Respond
http://contact.ebay.com/ws
M2MContact&item=330216
d=mhj7&qid=38166671O&r
Name=ADME:X:AAO:US:113


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
d1taylor
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

How well does it work?

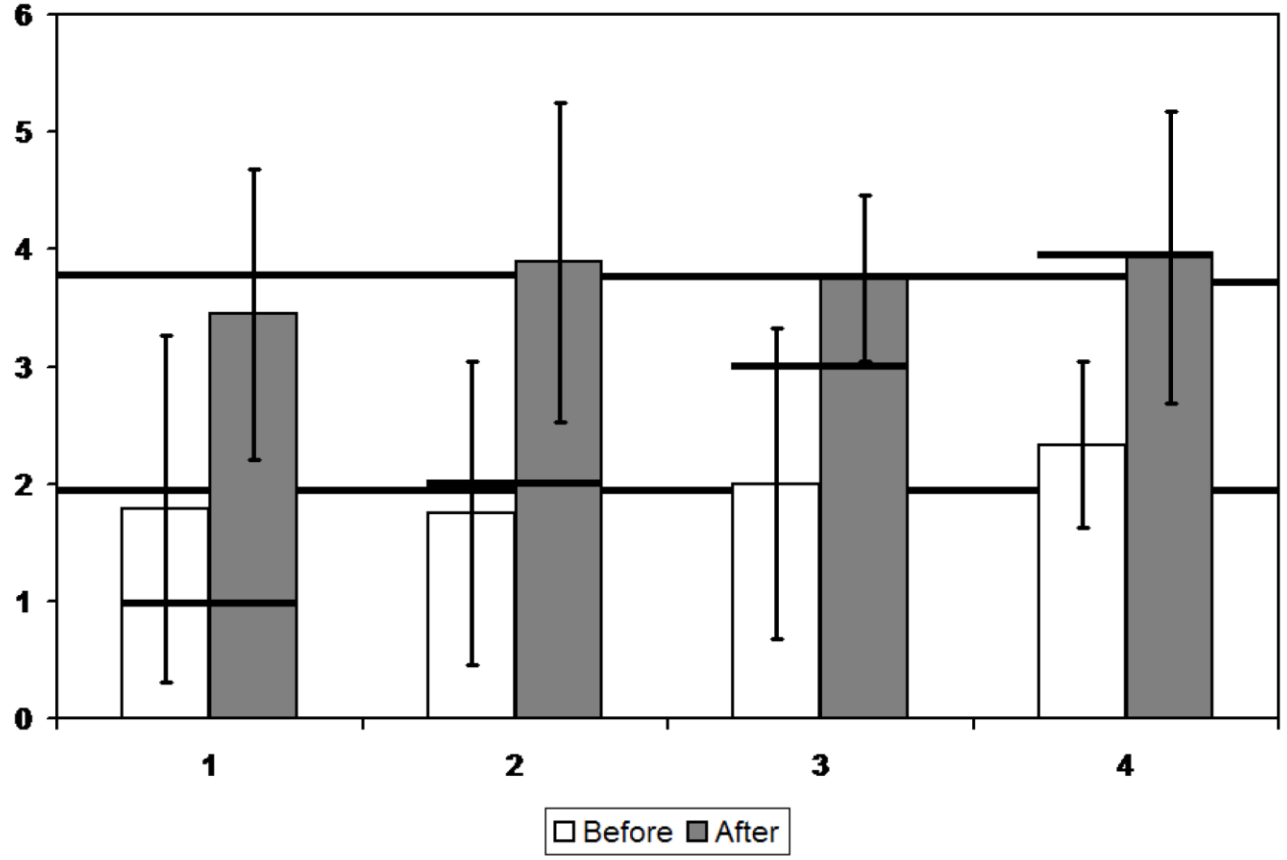
- Cost: $80 / 1 million emails
  - Something like 10K-30K users will visit your site
- Success rate in the wild: ?
  - Fraction of users who type in credentials: ?
- Gartner: $2.4 billion/year in losses, 19% of Americans have clicked on a link in a phishing email, 3% have disclosed credentials

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 saying "There was a problem with your last grade report; click here to resolve it." 80% clicked.

Let’s look at some potential defenses….

Phishing education?



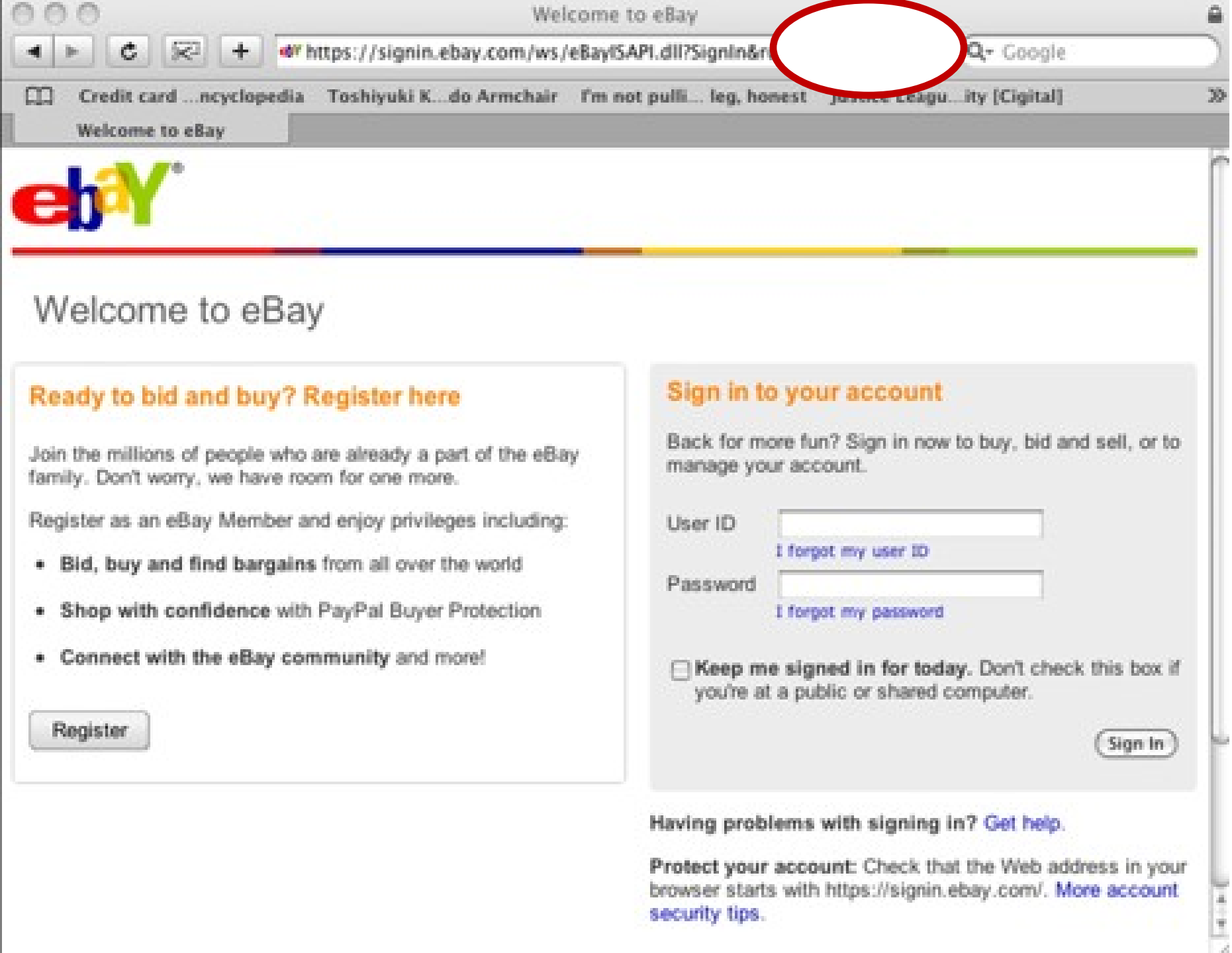
x-axis = Number of emails that were phish

y-axis = Number of emails classified by users as phish

Check the URL before clicking?

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

Check the URL in address bar?


Welcome to eBay
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&r
Google
Credit card ...ncyclopedia
Toshiyuki K...do Armchair
I'm not pulli... leg, honest
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.

Personal Banking - PNC Bank - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pnc.com/webapp/unsec/homepag

Google

Most Visited Getting Started Latest Headlines

PNC
LEADING THE WAY

HOME SECURITY ASSURANCE LOCATE PNC CONTACT US CUSTOMER SERVI

Search

PERSONAL SMALL BUSINESS CORPORATE & INSTITUTIONAL ABOUT PNC

Online Banking Sign On

User ID: 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

PNC Security Assurance

Products and Services

Solutions

FDIC

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

Done

Homograph Attacks

- International domain names can use international character set
  - Chinese contains characters that look like / . ? =
- **Attack**: Register var.cn, buy wildcard cert for *.var.cn, then create a subdomain:

  www.pnc.com/webapp/unsec/homepage.var.cn

Check for padlock?

Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.wachovia.com/

WACHOVIA

Wac

Our comm

LOGI

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

En e

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...

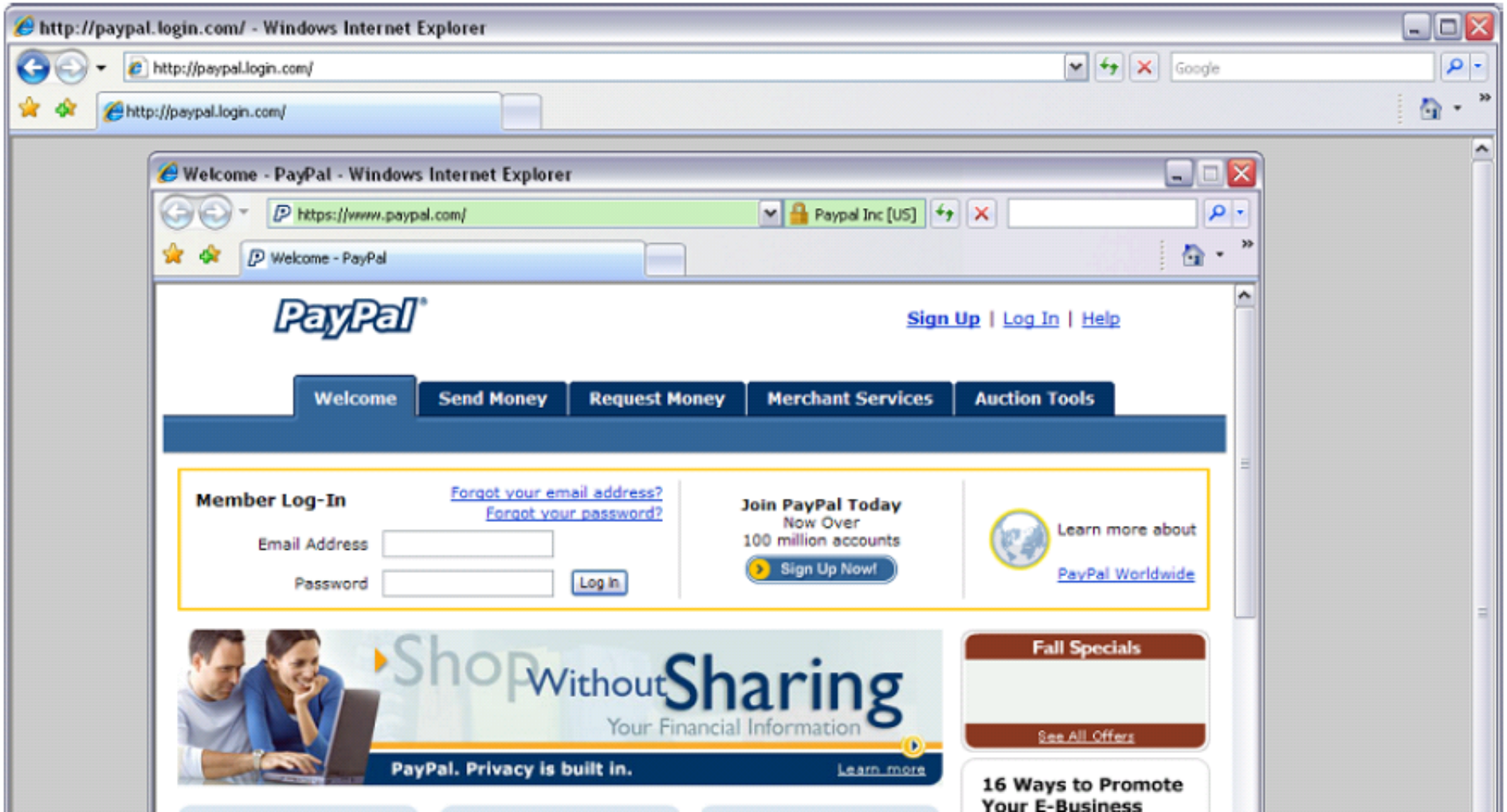
Lending
Mortgage
Home Equity **New!**
Education Loans
Vehicle Loans

Rates
Mortgage Rates

Add a clever .favicon with a picture of a padlock

Check for “green glow” in address bar?

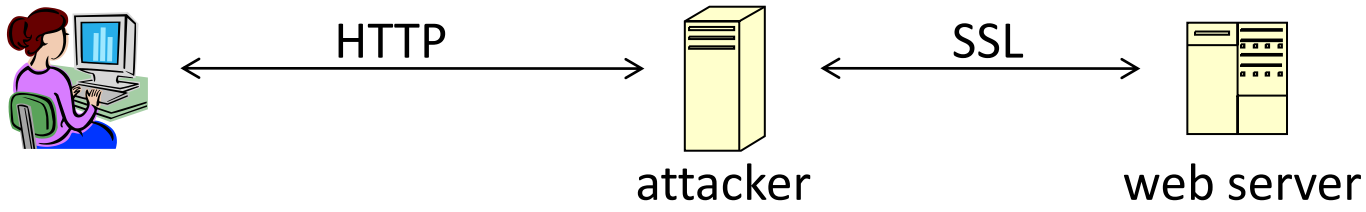
Check for everything?


http://paypal.login.com/ - Windows Internet Explorer
http://paypal.login.com/
Google
http://paypal.login.com/
Welcome - PayPal - Windows Internet Explorer
https://www.paypal.com/
Paypal Inc [US]
Welcome - PayPal
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Services
Auction Tools
Member Log-In
Forgot your email address?
Forgot your password?
Email Address
Password
Log In
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.
Learn more
Fall Specials
See All Offers
16 Ways to Promote
Your E-Business

HTTP downgrade attacks

Common use pattern: Main page uses HTTP; change to HTTPS for secure login.

MITM Attack: prevent the upgrade [Moxie'08]



Which is real? Which is the attack?

8\6 7DZ DQ%XVLQHVV&RXQFLO

FrRm: US-Taiwan Business Council [council@us-taiwan.org]
6HQt: Tuesday, January 16, 2007 9:54 AM
7R: [redacted]@state.gov
6XbjHFt: US-Taiwan Business Council Defense & Security Bulletin

The Defense & Security Bulletin is attached in DOC format.

Table of Contents

DEFENSE AND SECURITY
1. Biometric Plan Aimed for National Security: Official
2. US, Japan to Discuss Taiwan's Defense
3. Taiwan Sees Red Over White Paper
4. KMT Plans to Send Arms Budget Back to Ministry
5. Use Fast Rail for Military: DPP AEROSPACE
6. CAA Mulls Transferring Charters to Taipei Airport
7. Current Exchange Rate
8. News Sources

****
US-Taiwan Business Council
1700 North Moore Street, Suite 1703
Arlington, Virginia 22209
Phone: (703) 465-2930
Fax: (703) 465-2937
council@us-taiwan.org

If you would like to unsubscribe from our mailing list, change your subscription preferences, or update your contact information, please contact the Council via email at update@us-taiwan.org. Visit us online at www.us-taiwan.org!
****

8\6 7DZ DQ%XVLQHVV&RXQFLO

FrRm: US-Taiwan Business Council [council@us-taiwan.org]
6HQt: Tuesday, January 09, 2007 4:59 PM
7R: 'council@us-taiwan.org'
6XbjHFt: US-Taiwan Business Council - 01.09.2007 - Defense & Security Bulletin

The Defense & Security Bulletin is attached in PDF format.

Table of Contents

DEFENSE AND SECURITY
1. Biometric Plan Aimed for National Security: Official
2. US, Japan to Discuss Taiwan's Defense
3. Taiwan Sees Red Over White Paper
4. KMT Plans to Send Arms Budget Back to Ministry
5. Use Fast Rail for Military: DPP

AEROSPACE
6. CAA Mulls Transferring Charters to Taipei Airport

7. Current Exchange Rate
8. News Sources

****
US-Taiwan Business Council
1700 North Moore Street, Suite 1703
Arlington, Virginia 22209
Phone: (703) 465-2930
Fax: (703) 465-2937
council@us-taiwan.org

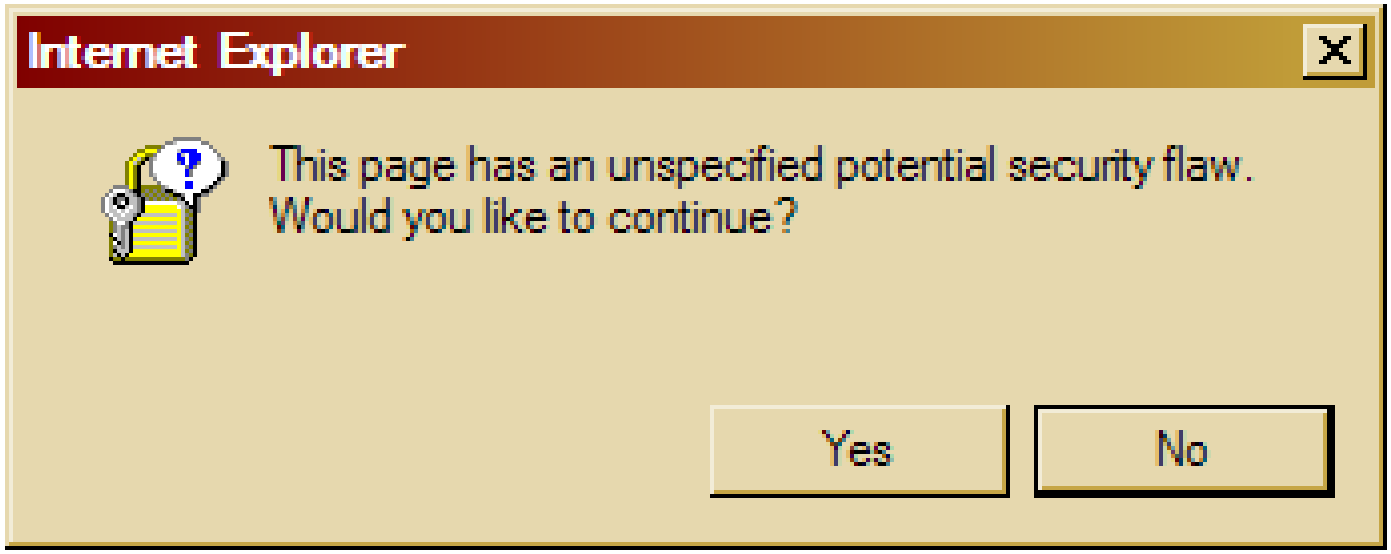
If you would like to unsubscribe from our mailing list, change your subscription preferences, or update your contact information, please contact the Council via email at update@us-taiwan.org. Visit us online at www.us-taiwan.org!
****

Why does phishing work?

Why does phishing work?

- User mental model ≠ 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
  - Psychology: people prefer to gamble for a chance of no loss than a sure loss

Warnings


Internet Explorer
This page has an unspecified potential security flaw.
Would you like to continue?
Yes
No

Certificate errors

What should you do if you see a SSL certificate error?

- Continue on to the site and ignore the error?
- Forget about visiting the site?

What if I told you that 62% of SSL-enabled websites have invalid certs?

Usable Security Ain't Easy

- You are not like the average user
  - The more you know about security, the less representative of the user population you are!
  - Your thought processes are very different from the average user (most CS folks have a **TJ personality types (INTJ is especially popular), but only 8% of population at large is **TJ).
- Your intuition is wrong!

Usable Security Ain't Easy

- Users' first priority is to get work done (not to think about security).
- Users satisfice.
- People usually use semi-instinctive learned processes – we are not rational puzzle-solvers, most of the time.

So how can we avoid these pitfalls?

- Understand the user population (anthropology). Understand human behavior (psychology).
- Perform user studies to test designs; expect to iterate through many designs.
- Avoid “blame transfer”. Don’t ask users to make decisions they don’t know how to make. Users are not the enemy.
- Design usability in from the start.