The Human Factor in Online Fraud

Annotated slides available at www.human-factor.org

Markus Jakobsson

Indiana University

markus@indiana.edu

Indiana University Cognitive Science Program

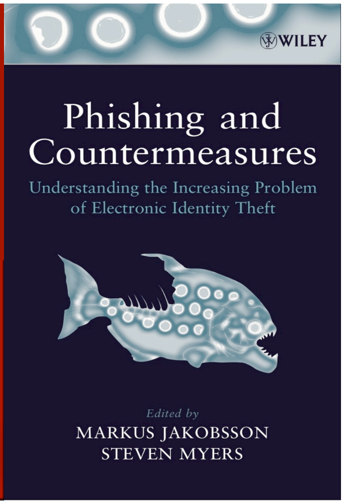
Indiana University School of informatics

RAVENWHITE

CACR

STOP-PHISHING.com

The Anti-Phishing group at Indiana University



WILEY

Phishing and Countermeasures

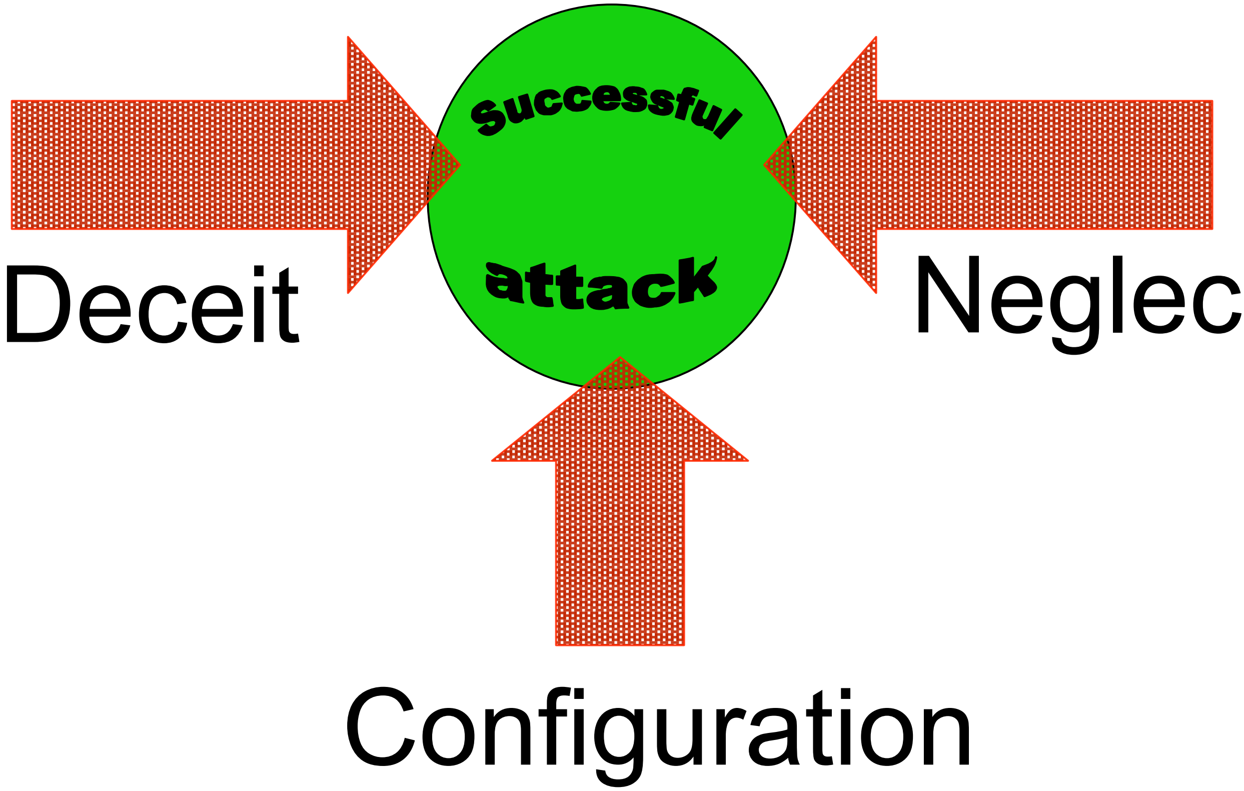
Understanding the Increasing Problem of Electronic Identity Theft

Edited by MARKUS JAKOBSSON STEVEN MYERS

Conventional Aspects of Security

- Computational assumptions
  - E.g., existence of a one-way function, RSA assumption, Decision Diffie-Hellman
- Adversarial model
  - E.g., access to data/hardware, ability to corrupt, communication assumptions, goals
- Verification methods
  - Cryptographic reductions to assumptions, BAN logic
- Implementation aspects
  - E.g., will the communication protocol leak information that is considered secret in the application layer?

The human factor of security



The human factor: configuration

Weak passwords

With Tsow, Yang, Wetzel: “Warkitting: the Drive-by Subversion of Wireless Home Routers”

(Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006)

Wireless firmware update

wardriving
rootkitting

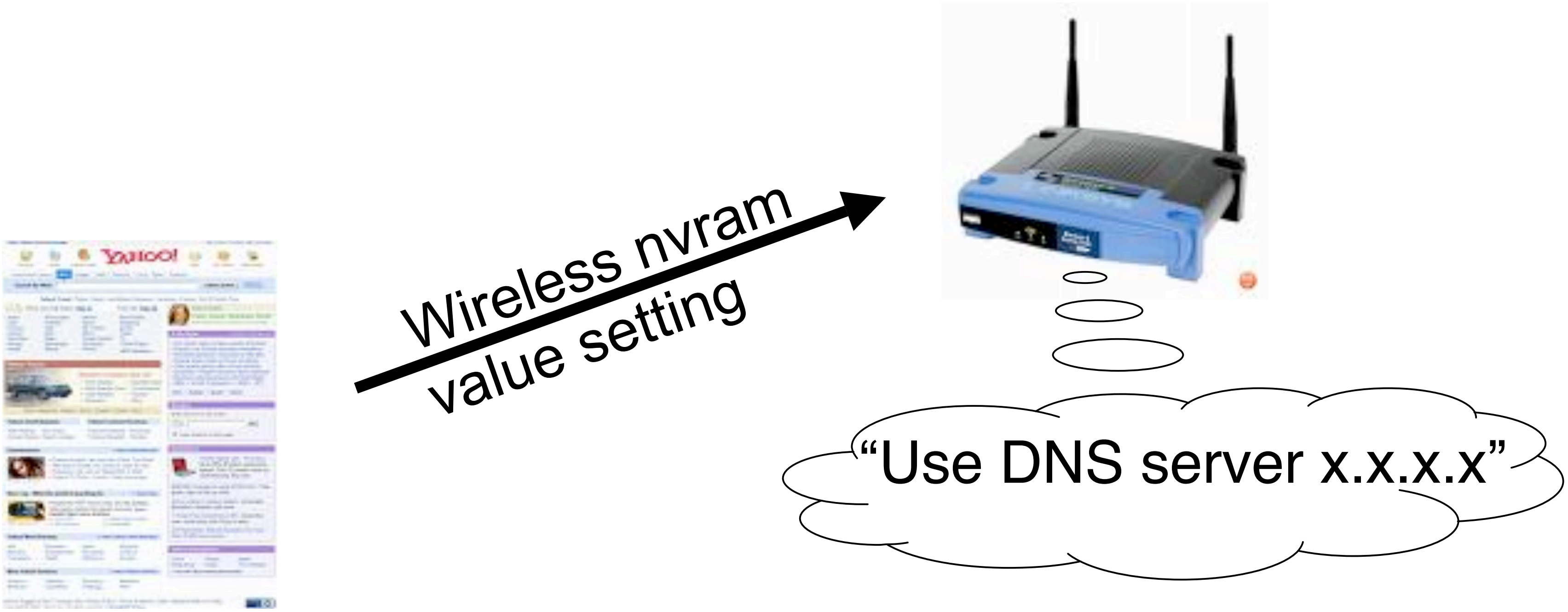
Shows that more than
50% of APs are vulnerable

The human factor: configuration

Weak passwords

With Stamm, Ramzan: “Drive-By Pharming”

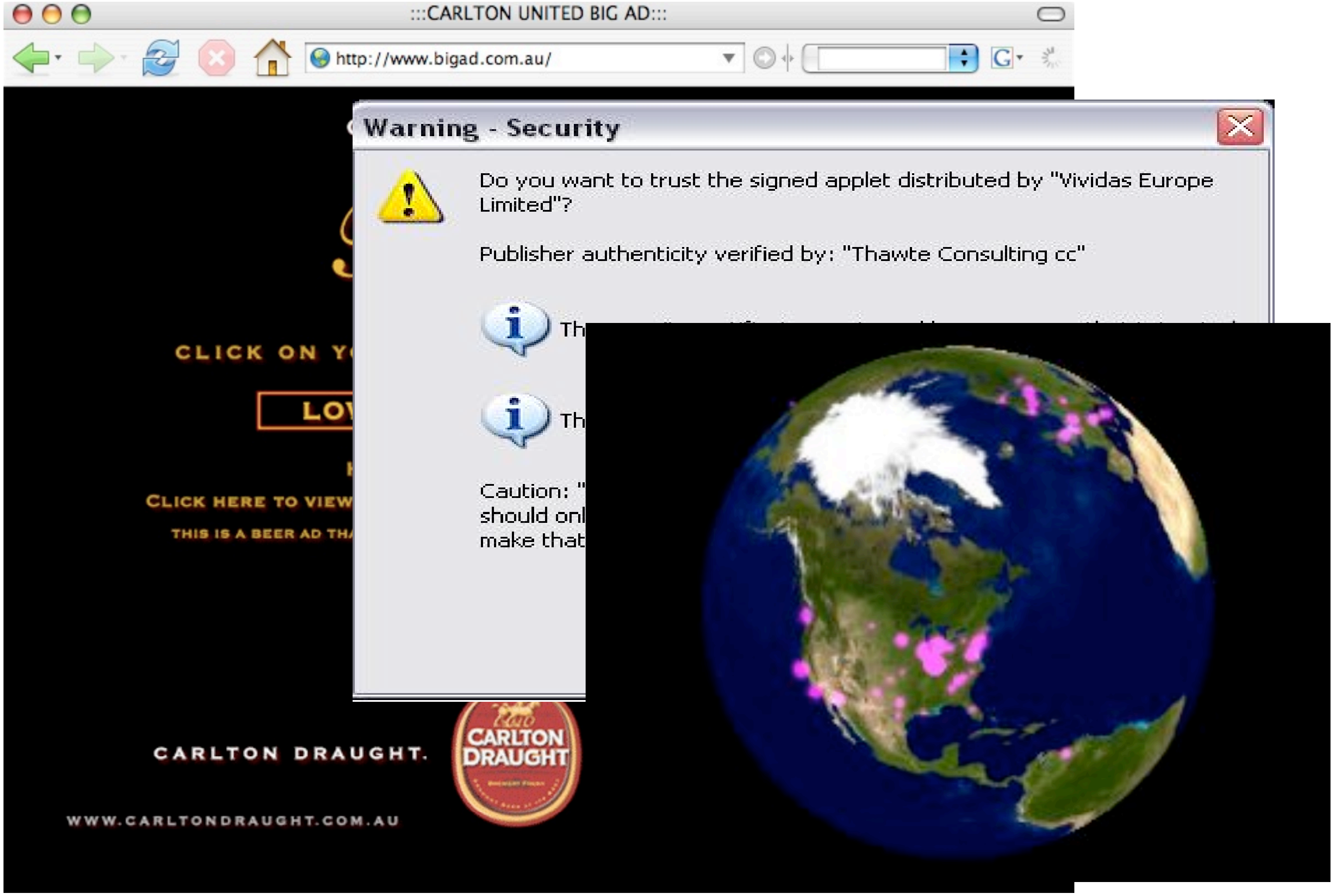
(Symantec press release, Feb 15, 2007; top story on Google Tech news on Feb 17; Cisco warns their 77 APs are vulnerable, Feb 21.)



Wireless nvram value setting

“Use DNS server x.x.x.x”

The human factor: neglect



Warning - Security

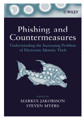
Do you want to trust the signed applet distributed by "Vividas Europe Limited"?

Publisher authenticity verified by: "Thawte Consulting cc"

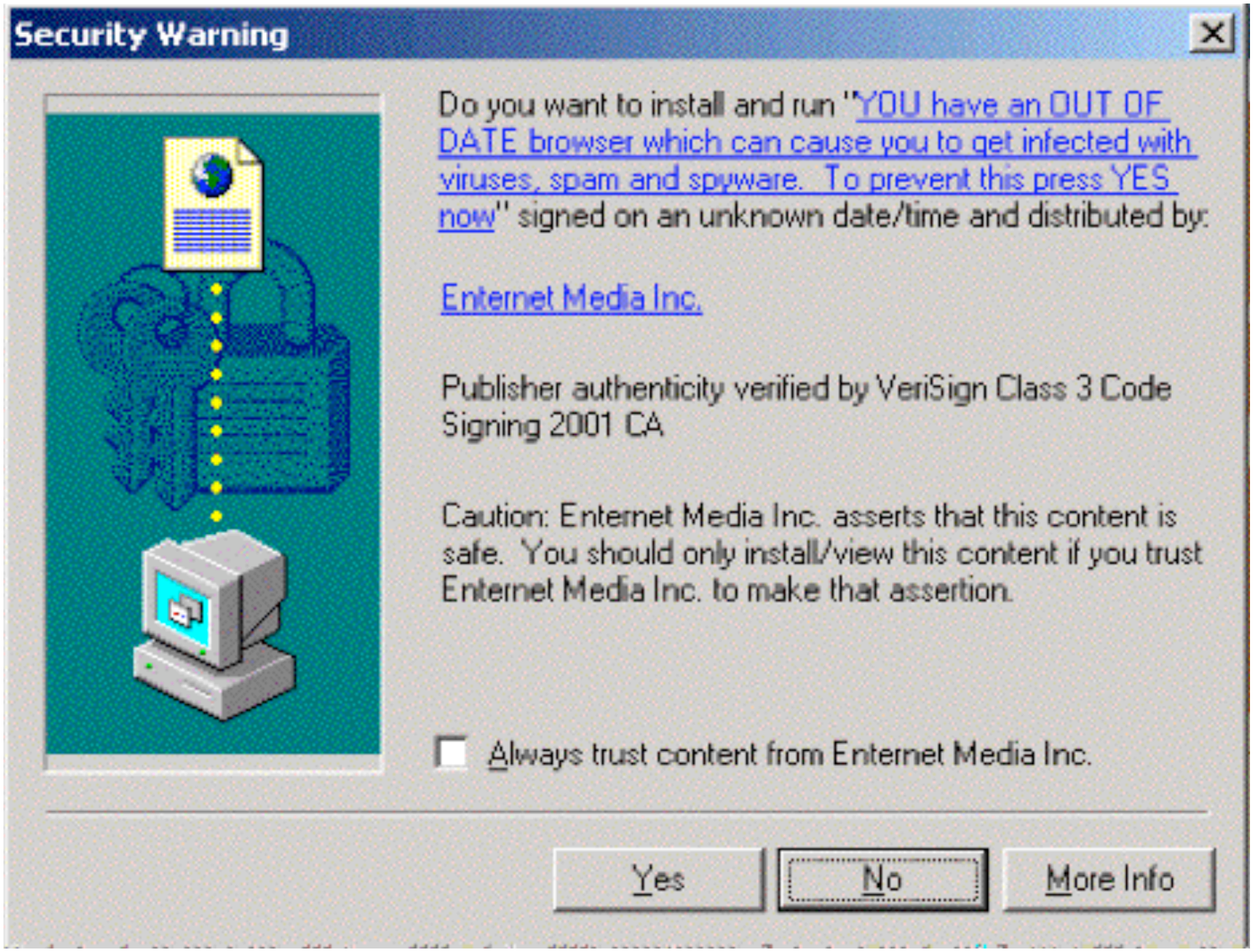
Th

Th

Caution: "
should onl
make that

With Stamm, Gandhi: “Socially Transmitted Malware”(in )

The human factor: deceit



Security Warning

Do you want to install and run "YOU have an OUT OF DATE browser which can cause you to get infected with viruses, spam and spyware. To prevent this press YES now" signed on an unknown date/time and distributed by:

Enternet Media Inc.

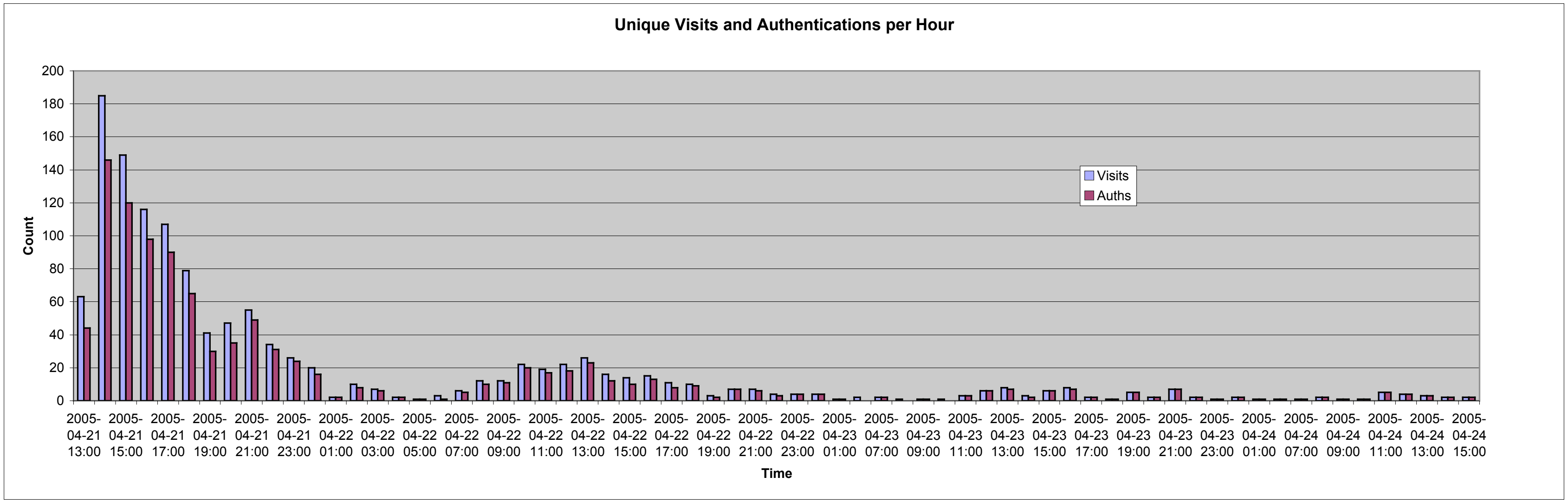
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: Enternet Media Inc. asserts that this content is safe. You should only install/view this content if you trust Enternet Media Inc. to make that assertion.

□ Always trust content from Enternet Media Inc.

(Threaten/disguise - image credit to Ben Edelman)

The human factor: deceit



Self: “Modeling and Preventing Phishing Attacks”

(Panel, Financial Crypto, 2005 - notion of spear phishing)

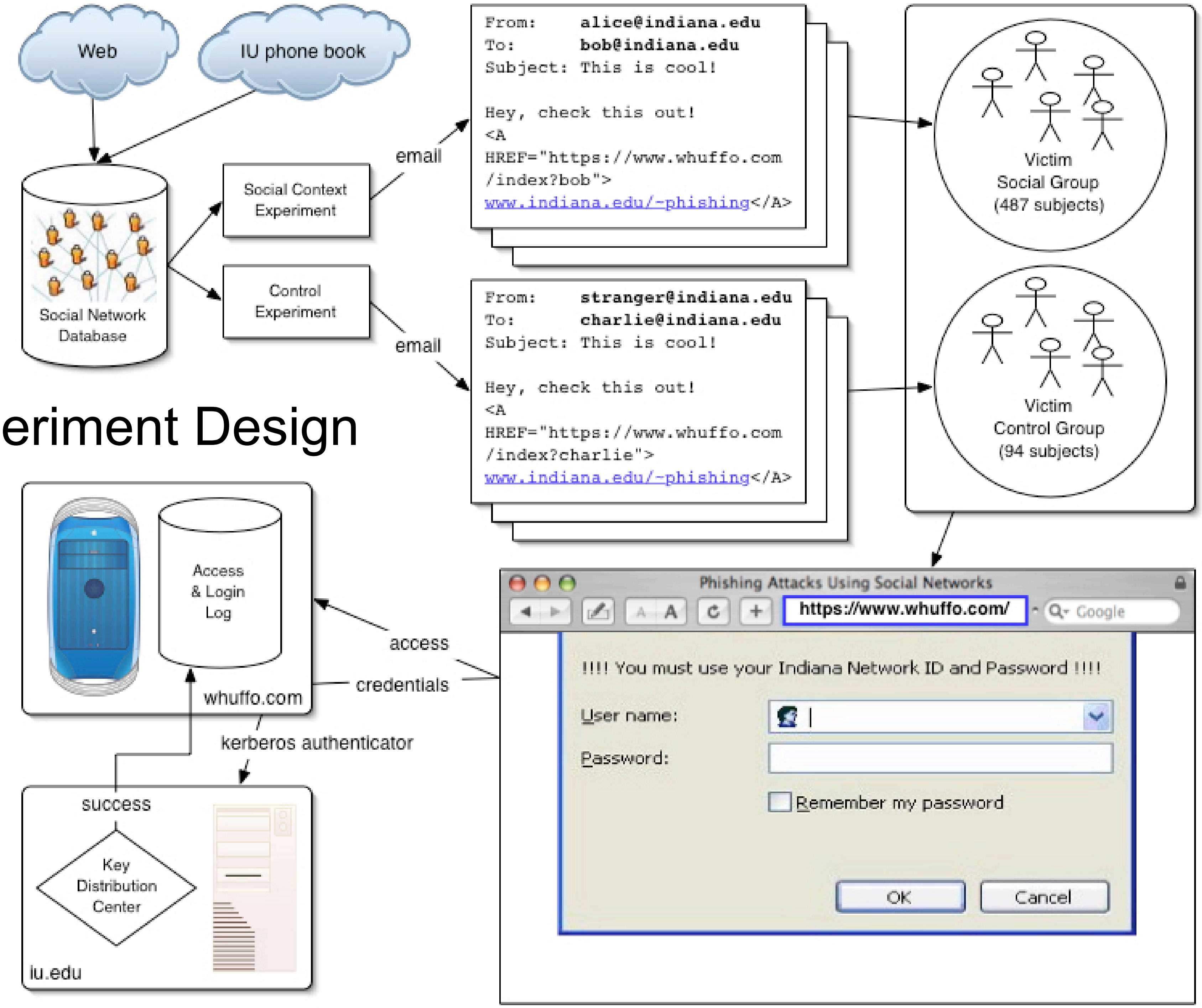
With Jagatic, Johnson, Menczer: “Social Phishing”

(To appear in the Communications of the ACM, Oct 2007)

Self: “The Human Factor of Phishing”

(Invited paper, Privacy & Security of Consumer Information, 2007)

Experiment Design



```
From:     alice@indiana.edu
To:       bob@indiana.edu
Subject: This is cool!

Hey, check this out!
<A
HREF="https://www.whuffo.com
/index?bob">
www.indiana.edu/~phishing</A>
```

```
From:     stranger@indiana.edu
To:       charlie@indiana.edu
Subject: This is cool!

Hey, check this out!
<A
HREF="https://www.whuffo.com
/index?charlie">
www.indiana.edu/~phishing</A>
```

https://www.whuffo.com/

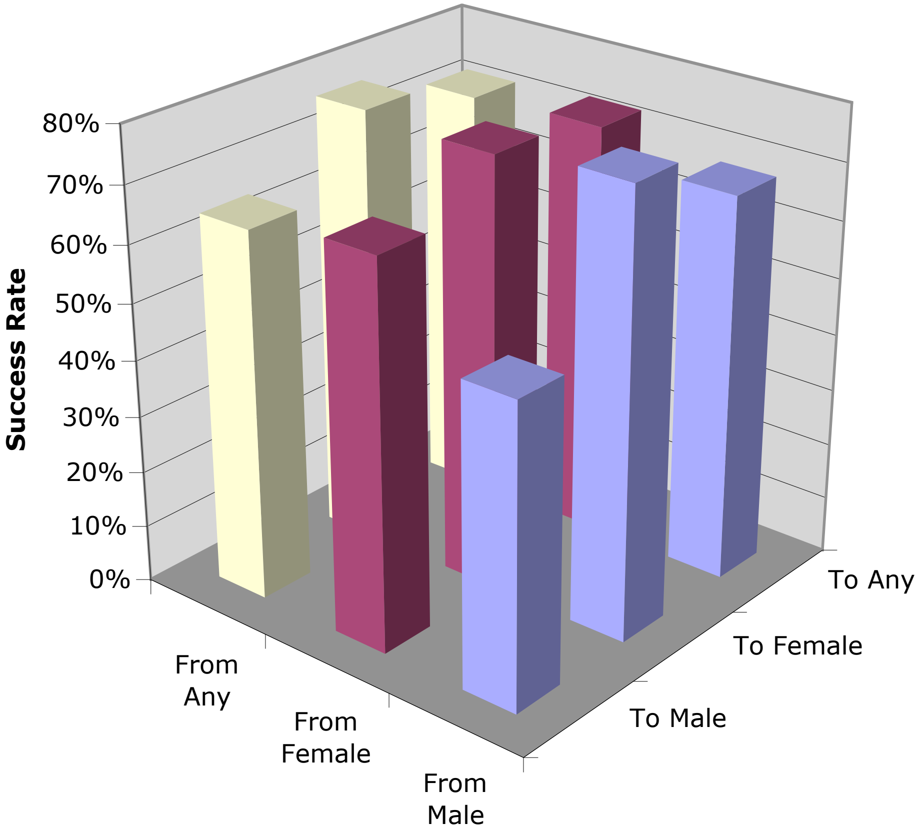
!!!! You must use your Indiana Network ID and Password !!!!

User name: |

Password:

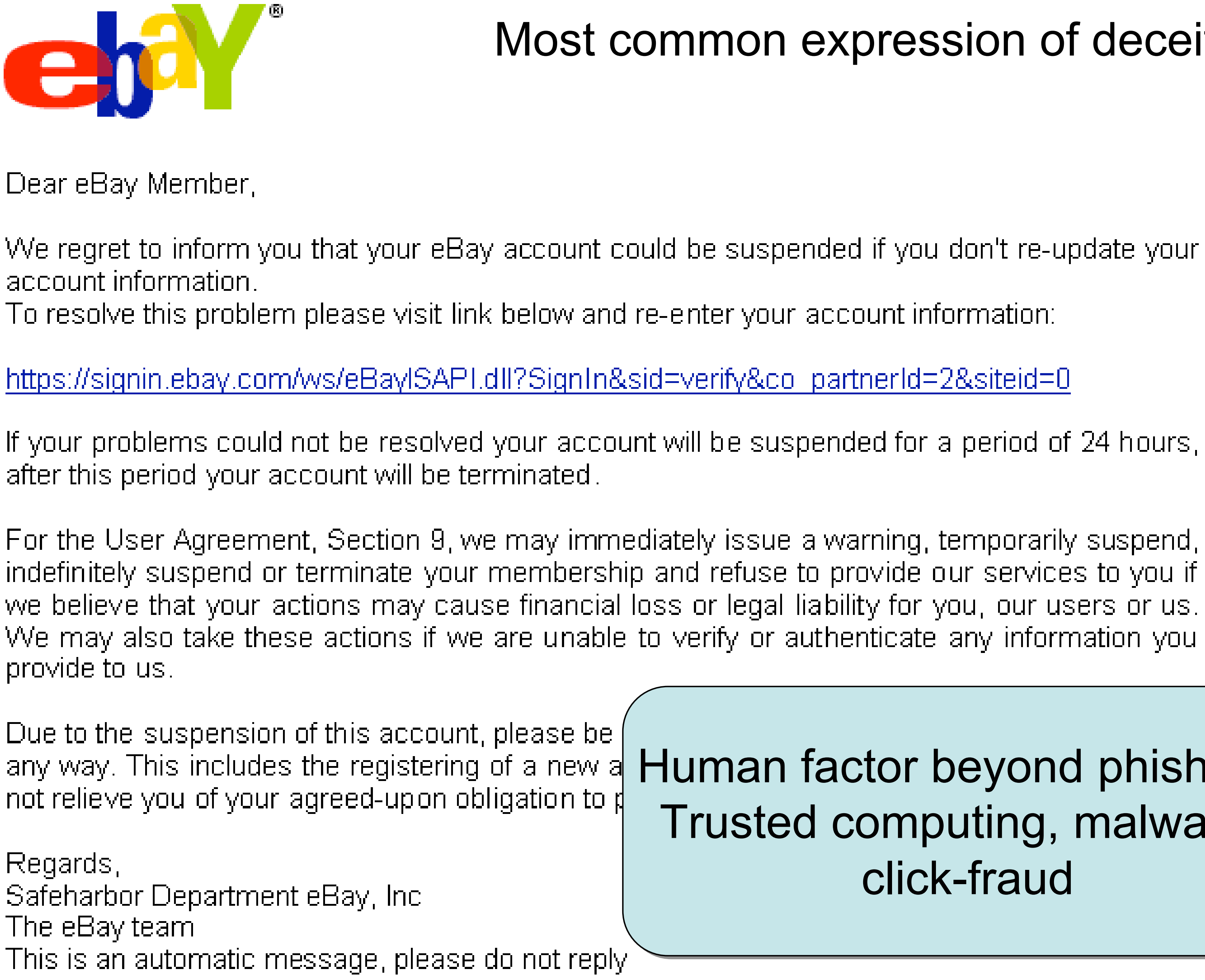
□ Remember my password

Gender Effects



	To Male	To Female	To Any
From Male	53%	78%	68%
From Female	68%	76%	73%
From Any	65%	77%	72%

Most common expression of deceit:



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

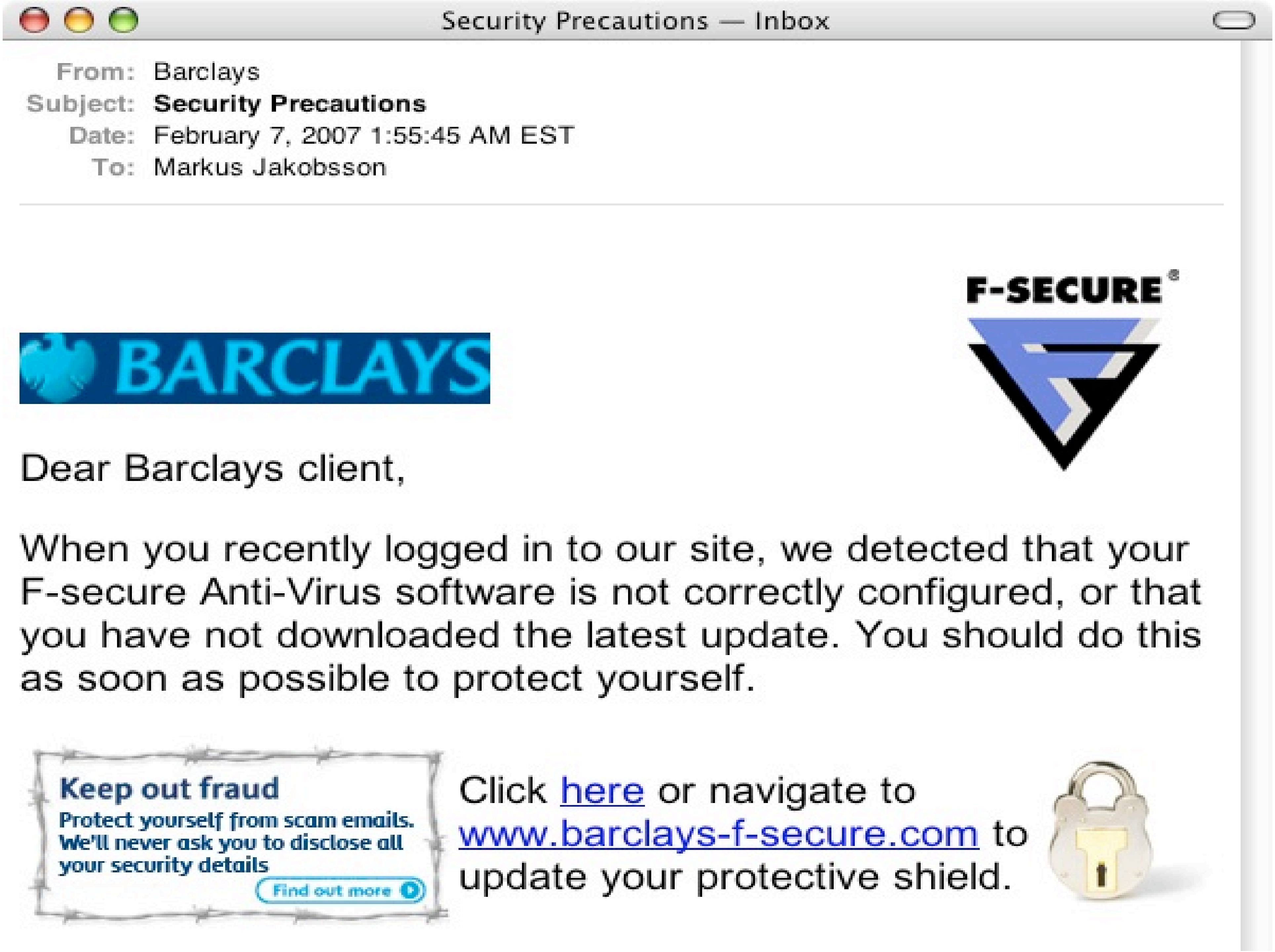
If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

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
any way. This includes the registering of a new a
not relieve you of your agreed-upon obligation to p

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

Human factor beyond phishing:
Trusted computing, malware, click-fraud



Security Precautions — Inbox

From: Barclays
Subject: **Security Precautions**
Date: February 7, 2007 1:55:45 AM EST
To: Markus Jakobsson

Dear Barclays client,

When you recently logged in to our site, we detected that your F-secure Anti-Virus software is not correctly configured, or that you have not downloaded the latest update. You should do this as soon as possible to protect yourself.

Keep out fraud
Protect yourself from scam emails. We'll never ask you to disclose all your security details

Click here or navigate to www.barclays-f-secure.com to update your protective shield.

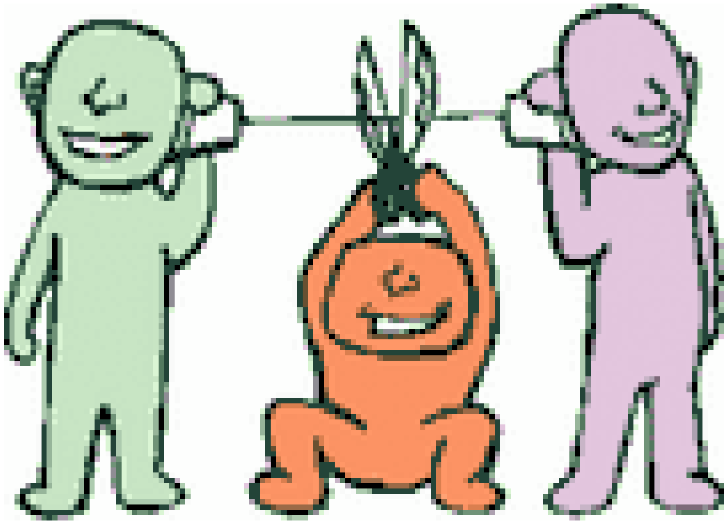
Spear Phishing and Data Mining

Current attack style:

Approx 3% of adult Americans report to have been victimized.

Spear Phishing and Data Mining

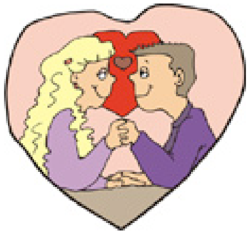
More sophisticated attack style:



“context aware attack”

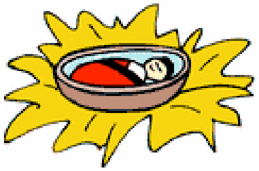
How can information be derived?

Jane Smith



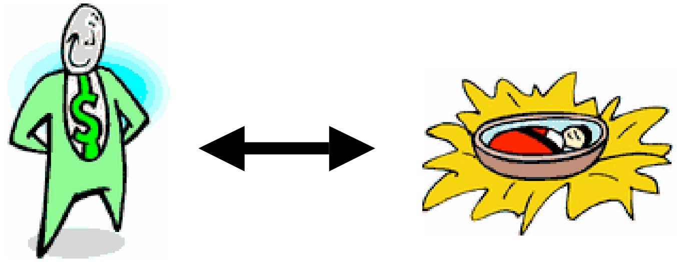
Jose Garcia

Jane Garcia, Jose Garcia



… and little Jimmy Garcia

Let’s start from the end!



“Little” Jimmy

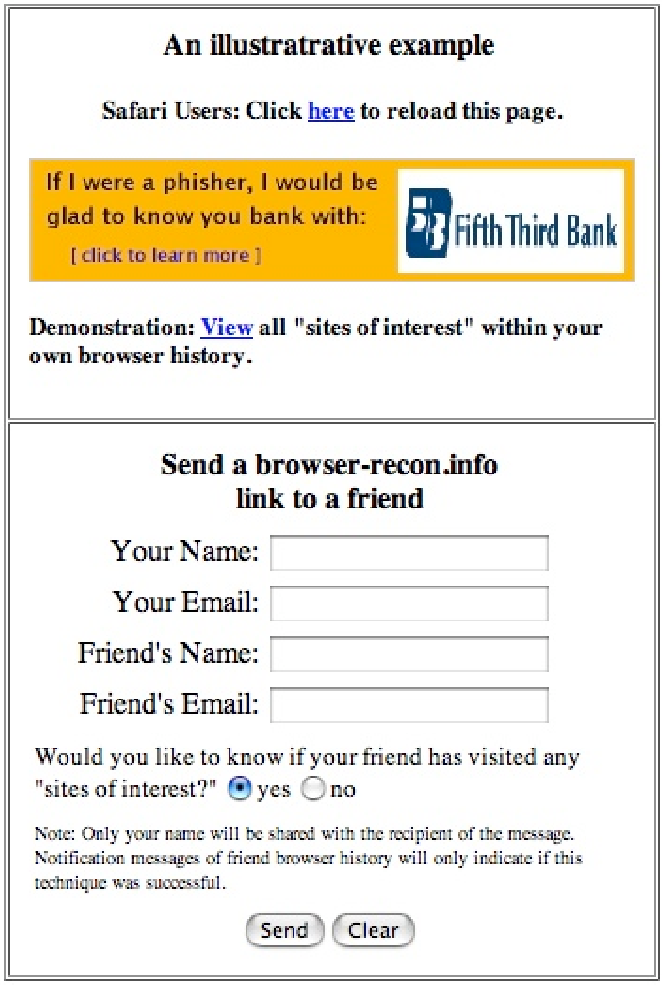
his parents

their marriage license

and Jimmy’s mother’s maiden name: Smith

More reading: Griffith and Jakobsson, "Messin' with Texas: Deriving Mother's Maiden Names Using Public Records."

www.browser-recon.info



An illustratrative example

Safari Users: Click here to reload this page.

If I were a phisher, I would be glad to know you bank with:

[click to learn more]

Demonstration: View all "sites of interest" within your own browser history.

Send a browser-recon.info link to a friend

Your Name:

Your Email:

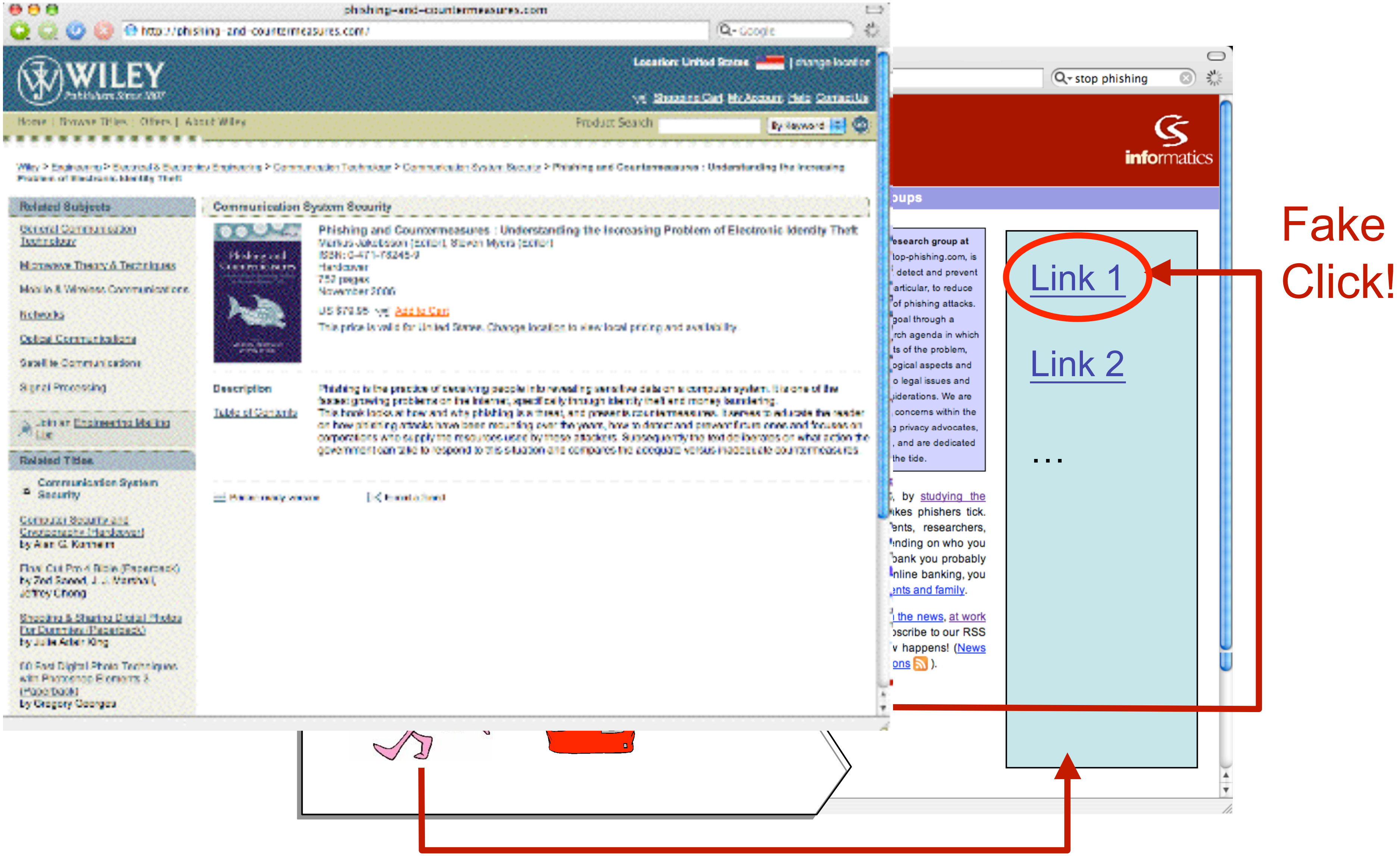
Friend's Name:

Friend's Email:

Would you like to know if your friend has visited any "sites of interest?" ● yes ○ no

Note: Only your name will be shared with the recipient of the message. Notification messages of friend browser history will only indicate if this technique was successful.

How to “auto-click”



phishing-and-countermeasures.com

http://phishing-and-countermeasures.com/

WILEY Publishers Since 1807

Location: United States | change location

Shopping Cart My Account Help Contact Us

Home | Browse Titles | Offers | About Wiley   Product Search   By Keyword

Wiley > Engineering > Electrical & Electronics Engineering > Communication Technologies > Communication System Security > Phishing and Countermeasures : Understanding the Increasing Problem of Electronic Identity Theft

Related Subjects

- General Communication Technology
- Microwave Theory & Techniques
- Mobile & Wireless Communications
- Networks
- Optical Communications
- Satellite Communications
- Signal Processing

Join an Engineering Mailing List

Related Titles

- Communication System Security
- Computer Security and Cryptography (Hardcover) by Alan G. Konheim
- Final Cut Pro 4 Bible (Paperback) by Zed Saeed, J. J. Marshall, Jeffrey Chong
- Shooting & Sharing Digital Photos For Dummies (Paperback) by Julie Adair King
- 50 Fast Digital Photo Techniques with Photoshop Elements 3 (Paperback) by Gregory Georges

Communication System Security

Phishing and Countermeasures : Understanding the Increasing Problem of Electronic Identity Theft
Markus Jakobsson (Editor), Steven Myers (Editor)
ISBN: 0-471-78245-9
Hardcover
752 pages
November 2006

US $79.95 Add to Cart

This price is valid for United States. Change location to view local pricing and availability.

Description

Table of Contents

Phishing is the practice of deceiving people into revealing sensitive data on a computer system. It is one of the fastest growing problems on the Internet, specifically through identity theft and money laundering. This book looks at how and why phishing is a threat, and presents countermeasures. It serves to educate the reader on how phishing attacks have been mounting over the years, how to detect and prevent future ones and focuses on corporations who supply the resources used by these attackers. Subsequently the text deliberates on what action the government can take to respond to this situation and compares the adequate versus inadequate countermeasures.

Printer-ready version   E-mail a friend

stop phishing

informatics

oups

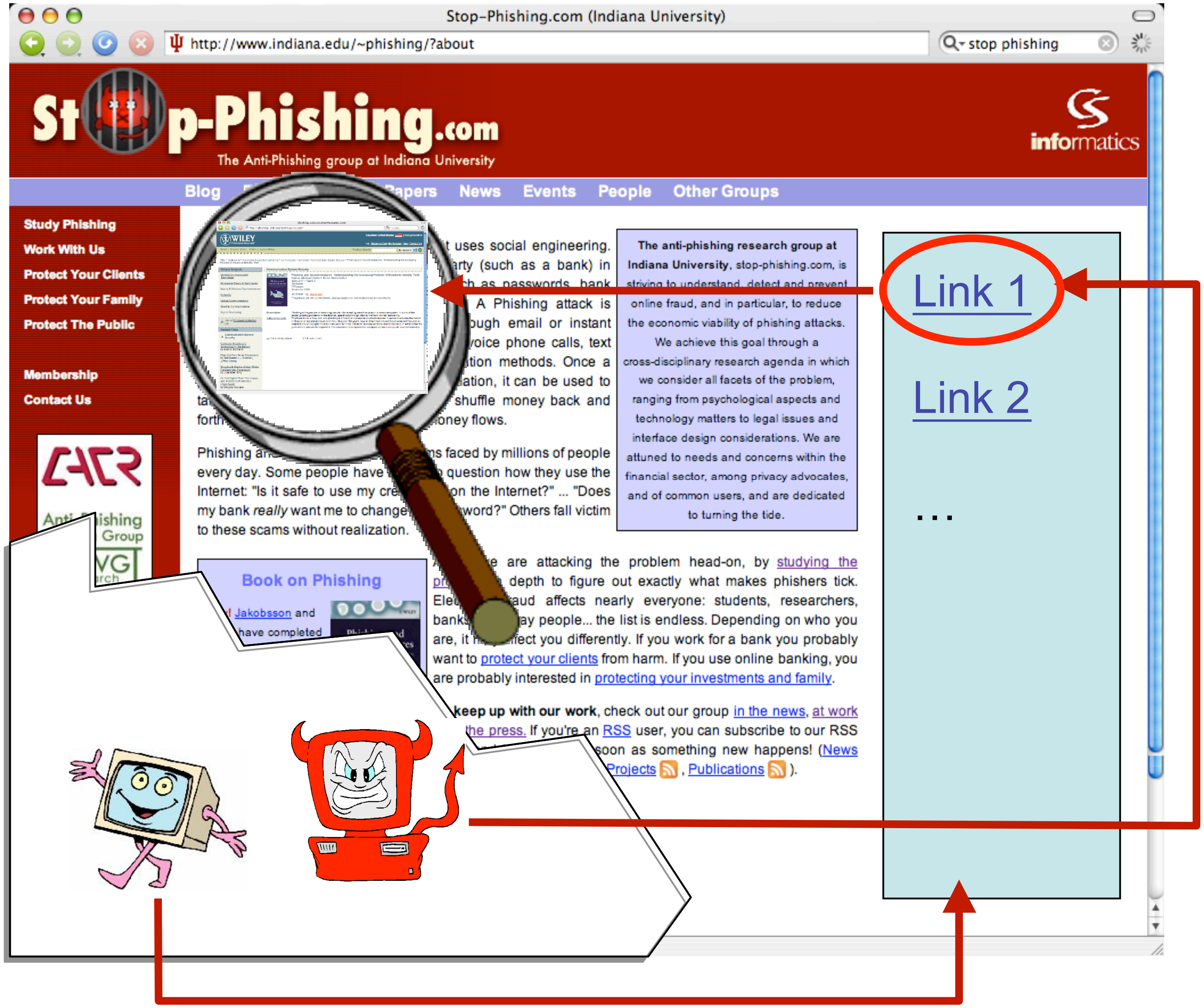
esearch group at top-phishing.com, is detect and prevent articular, to reduce of phishing attacks. goal through a rch agenda in which ts of the problem, ogical aspects and o legal issues and siderations. We are concerns within the g privacy advocates, , and are dedicated the tide.

, by studying the kes phishers tick. ents, researchers, nding on who you bank you probably nline banking, you ents and family.

the news, at work bscribe to our RSS v happens! (News ons).

Read from page (same domain!) and make URL request

Hiding it from the user



t uses social engineering. arty (such as a bank) in ch as passwords, bank A Phishing attack is ough email or instant voice phone calls, text tion methods. Once a ation, it can be used to ta shuffle money back and forth oney flows.

Phishing ar ns faced by millions of people every day. Some people have question how they use the Internet: "Is it safe to use my cre on the Internet?" ... "Does my bank *really* want me to change word?" Others fall victim to these scams without realization.

The anti-phishing research group at Indiana University, stop-phishing.com, is striving to understand, detect and prevent online fraud, and in particular, to reduce the economic viability of phishing attacks. We achieve this goal through a cross-disciplinary research agenda in which we consider all facets of the problem, ranging from psychological aspects and technology matters to legal issues and interface design considerations. We are attuned to needs and concerns within the financial sector, among privacy advocates, and of common users, and are dedicated to turning the tide.

Book on Phishing

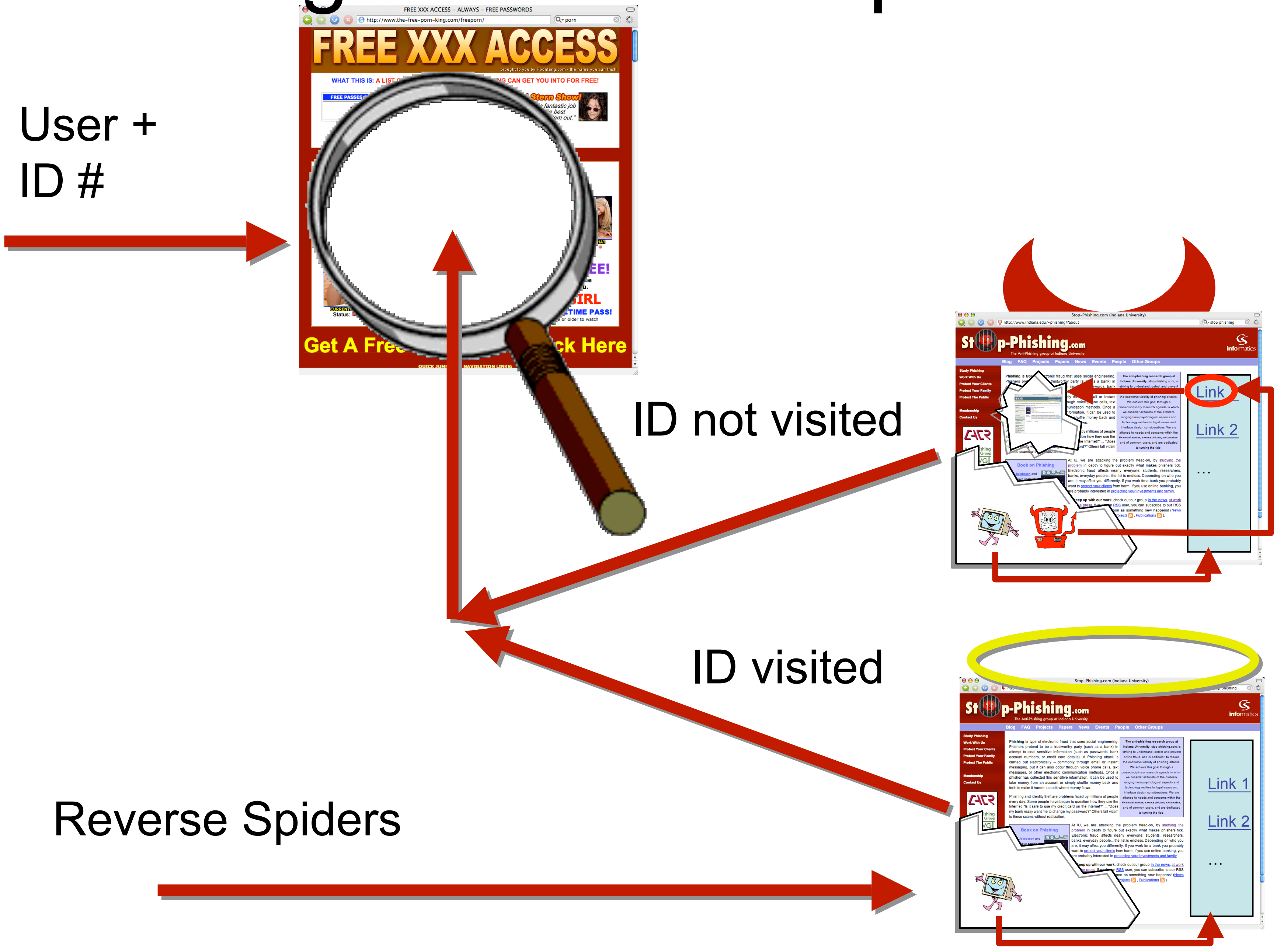
! Jakobsson and have completed

e are attacking the problem head-on, by studying the pr depth to figure out exactly what makes phishers tick. Ele aud affects nearly everyone: students, researchers, banks ay people... the list is endless. Depending on who you are, it ffect you differently. If you work for a bank you probably want to protect your clients from harm. If you use online banking, you are probably interested in protecting your investments and family.

keep up with our work, check out our group in the news, at work the press. If you're an RSS user, you can subscribe to our RSS soon as something new happens! (News Projects , Publications).

Fake Click!

Hiding from service providers



User +
ID #

ID not visited

ID visited

Reverse Spiders

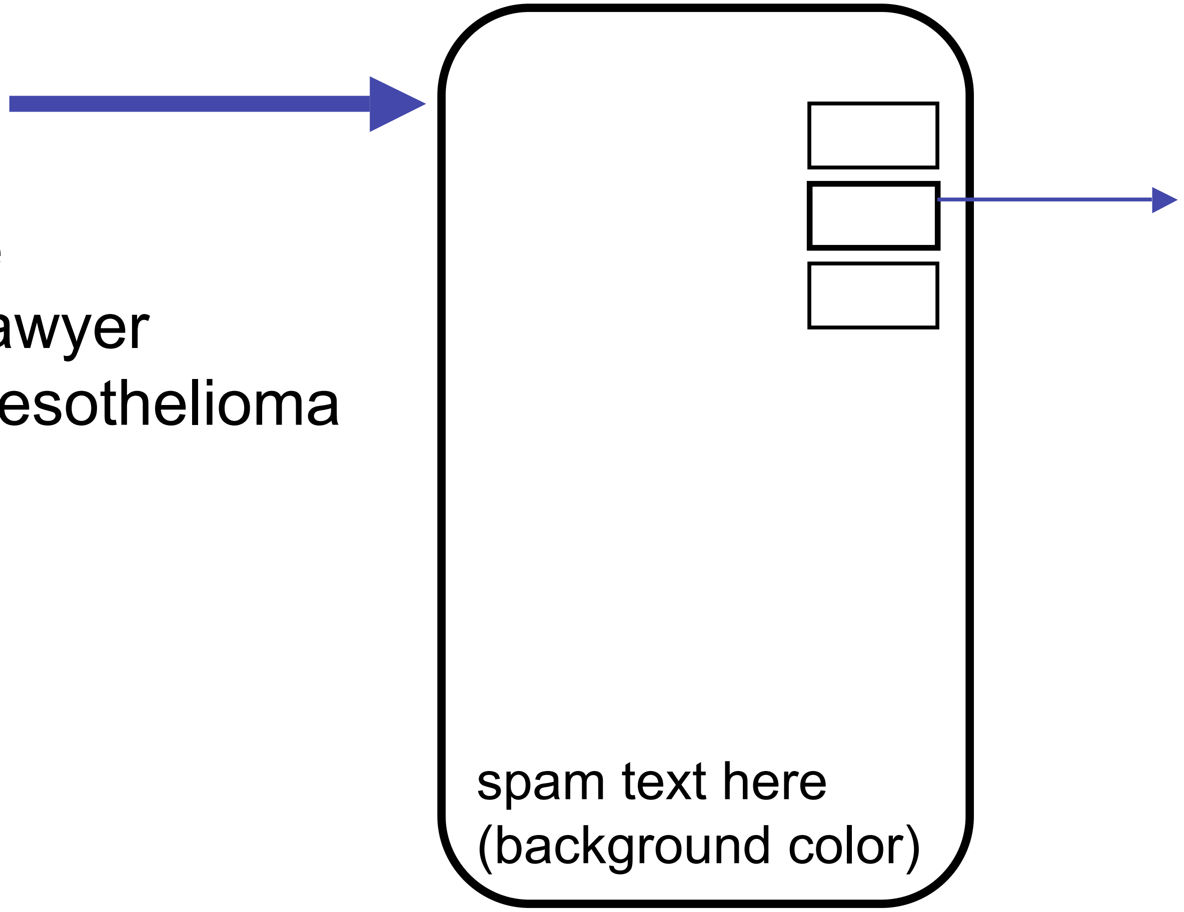
Avoiding screening of bad js

```
for( i= 1; i <= 10; i++ ){
document.write( i );}
```

```
code = "f@o"+"#r(i@"+"#="+1+";@"+"i#<=1%0"+";i"
+"+@#+){ @"+"d#oc"+"%um#"+"en%t."+"@w#r"
+"i#te"+"(@i + ¥"<b" + "r>¥");}";
eval(code.replace(/[@#%]/g, ""));
```

Possible attack: Using deceit

1. Legitimate
2. Attorney/lawyer
3. Asthma/mesothelioma



spam text here
(background color)

P k:

… and if you are interested in adfraud and how to stop it, consider attending AdFraud ‘07 (September 14, Palo Alto, CA)

Organizers:
Dan Boneh and Markus Jakobsson

1. Legit
2. Attor
3. Asthi

ere
(background color)

Big picture

Security & Crypto

Solve the right problem!

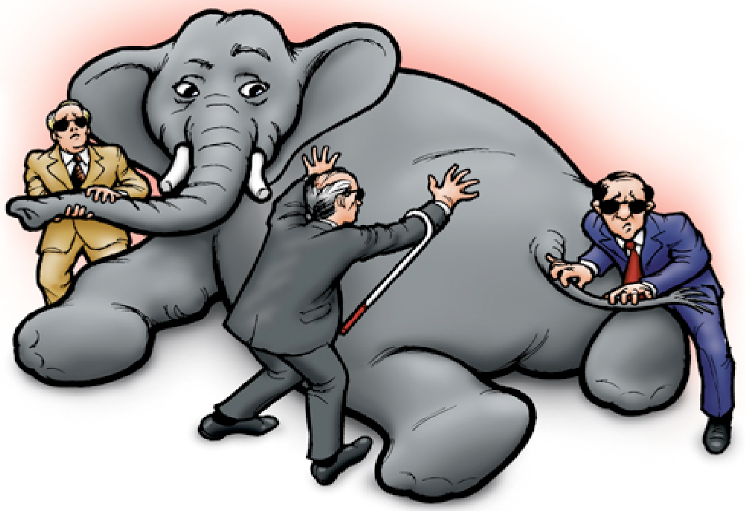
Psychology & HCI/D

Attackers follow law of least resistance.

Improved technology puts pressure on other technology.

Core belief

People are *people*, not machines.

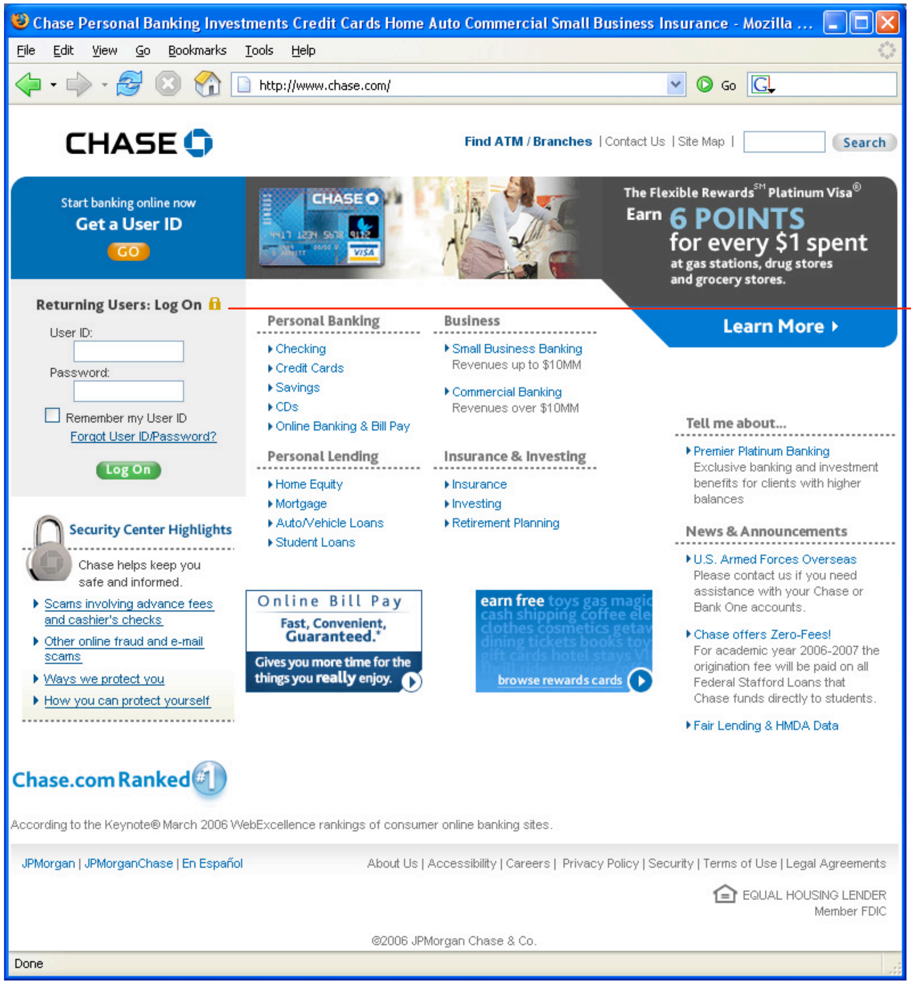


We need to measure vulnerabilities
(in-lab and naturalistically)
to understand the threat
and the efficacy of countermeasures.

Why do we need phishing experiments?

To improve phishing countermeasures, knowing what works and what does not.

Padlocks do not matter


Chase Personal Banking Investments Credit Cards Home Auto Commercial Small Business Insurance - Mozilla ...
File Edit View Go Bookmarks Tools Help
http://www.chase.com/
Go
CHASE
Search
GO
Log On
Done

Find ATM / Branches | Contact Us | Site Map |

Start banking online now
Get a User ID

The Flexible Rewards℠ Platinum Visa®
Earn 6 POINTS for every $1 spent at gas stations, drug stores and grocery stores.
Learn More

Returning Users: Log On

User ID:

Password:

□ Remember my User ID

Forgot User ID/Password?

Personal Banking
- Checking
- Credit Cards
- Savings
- CDs
- Online Banking & Bill Pay

Business
- Small Business Banking
  Revenues up to $10MM
- Commercial Banking
  Revenues over $10MM

Personal Lending
- Home Equity
- Mortgage
- Auto/Vehicle Loans
- Student Loans

Insurance & Investing
- Insurance
- Investing
- Retirement Planning

Tell me about...
- Premier Platinum Banking
  Exclusive banking and investment benefits for clients with higher balances

News & Announcements
- U.S. Armed Forces Overseas
  Please contact us if you need assistance with your Chase or Bank One accounts.
- Chase offers Zero-Fees!
  For academic year 2006-2007 the origination fee will be paid on all Federal Stafford Loans that Chase funds directly to students.
- Fair Lending & HMDA Data

Security Center Highlights

Chase helps keep you safe and informed.
- Scams involving advance fees and cashier's checks
- Other online fraud and e-mail scams
- Ways we protect you
- How you can protect yourself

Online Bill Pay
Fast, Convenient, Guaranteed.*
Gives you more time for the things you really enjoy.

earn free toys gas magic cash shipping coffee ele clothes cosmetics getav dining tickets books toy gift cards hotel stays
browse rewards cards

Chase.com Ranked #1

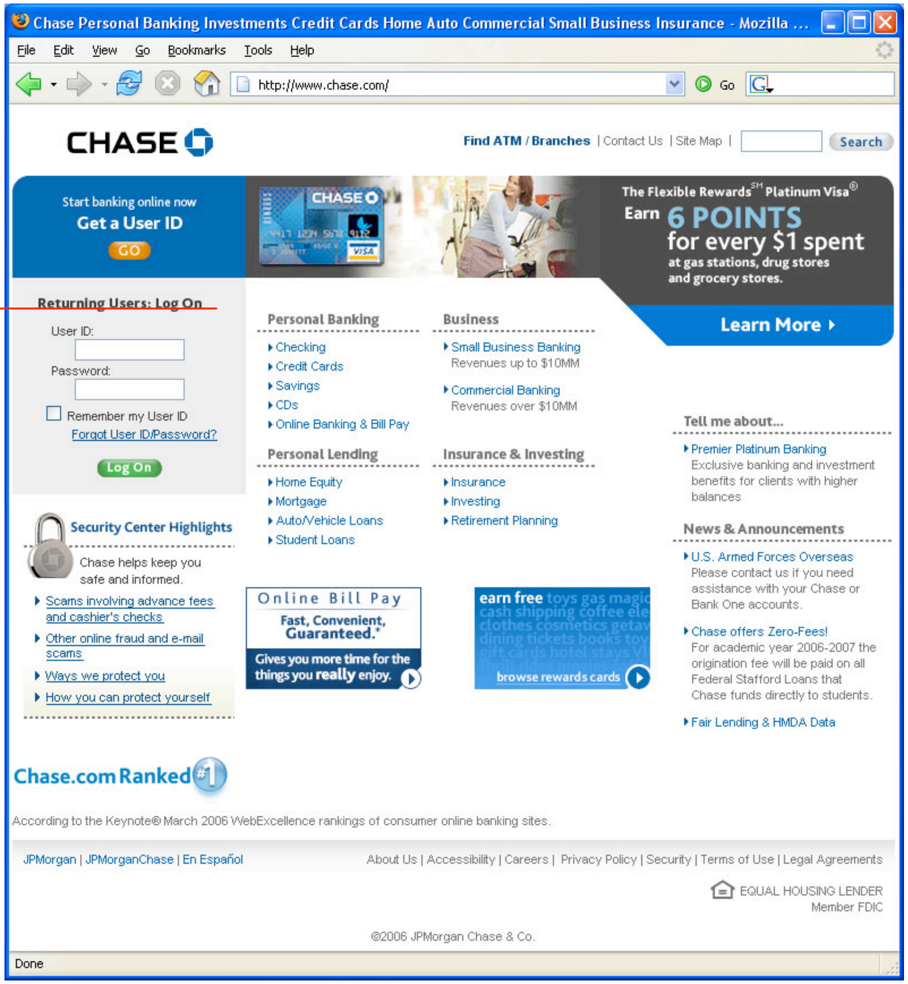
According to the Keynote® March 2006 WebExcellence rankings of consumer online banking sites.

JPMorgan | JPMorganChase | En Español

About Us | Accessibility | Careers | Privacy Policy | Security | Terms of Use | Legal Agreements

EQUAL HOUSING LENDER
Member FDIC

©2006 JPMorgan Chase & Co.


Chase Personal Banking Investments Credit Cards Home Auto Commercial Small Business Insurance - Mozilla ...
File Edit View Go Bookmarks Tools Help
http://www.chase.com/

Find ATM / Branches | Contact Us | Site Map |

Start banking online now
Get a User ID

The Flexible Rewards℠ Platinum Visa®
Earn 6 POINTS for every $1 spent at gas stations, drug stores and grocery stores.
Learn More

Returning Users: Log On

User ID:

Password:

□ Remember my User ID

Forgot User ID/Password?

Personal Banking
- Checking
- Credit Cards
- Savings
- CDs
- Online Banking & Bill Pay

Business
- Small Business Banking
  Revenues up to $10MM
- Commercial Banking
  Revenues over $10MM

Personal Lending
- Home Equity
- Mortgage
- Auto/Vehicle Loans
- Student Loans

Insurance & Investing
- Insurance
- Investing
- Retirement Planning

Tell me about...
- Premier Platinum Banking
  Exclusive banking and investment benefits for clients with higher balances

News & Announcements
- U.S. Armed Forces Overseas
  Please contact us if you need assistance with your Chase or Bank One accounts.
- Chase offers Zero-Fees!
  For academic year 2006-2007 the origination fee will be paid on all Federal Stafford Loans that Chase funds directly to students.
- Fair Lending & HMDA Data

Security Center Highlights

Chase helps keep you safe and informed.
- Scams involving advance fees and cashier's checks
- Other online fraud and e-mail scams
- Ways we protect you
- How you can protect yourself

Online Bill Pay
Fast, Convenient, Guaranteed.*
Gives you more time for the things you really enjoy.

earn free toys gas magic cash shipping coffee ele clothes cosmetics getav dining tickets books toy gift cards hotel stays
browse rewards cards

Chase.com Ranked #1

According to the Keynote® March 2006 WebExcellence rankings of consumer online banking sites.

JPMorgan | JPMorganChase | En Español

About Us | Accessibility | Careers | Privacy Policy | Security | Terms of Use | Legal Agreements

EQUAL HOUSING LENDER
Member FDIC

©2006 JPMorgan Chase & Co.

Done

(Clean) URLs matter

https://www.accountonline.com/View?DocId=Index\&siteId=AC\&langID=EN

significantly less (with $p<0.004$) trustworthy than

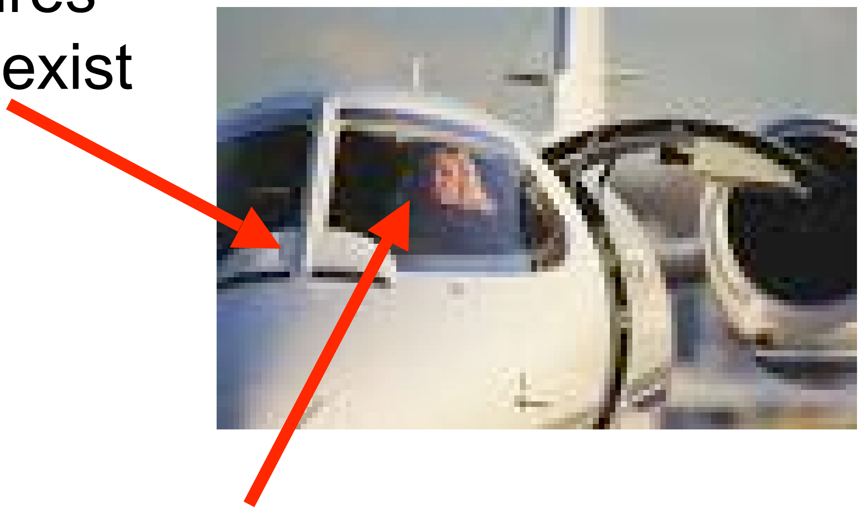
http://www.attuniversalcard.com

Why do we need phishing experiments?

To improve security education

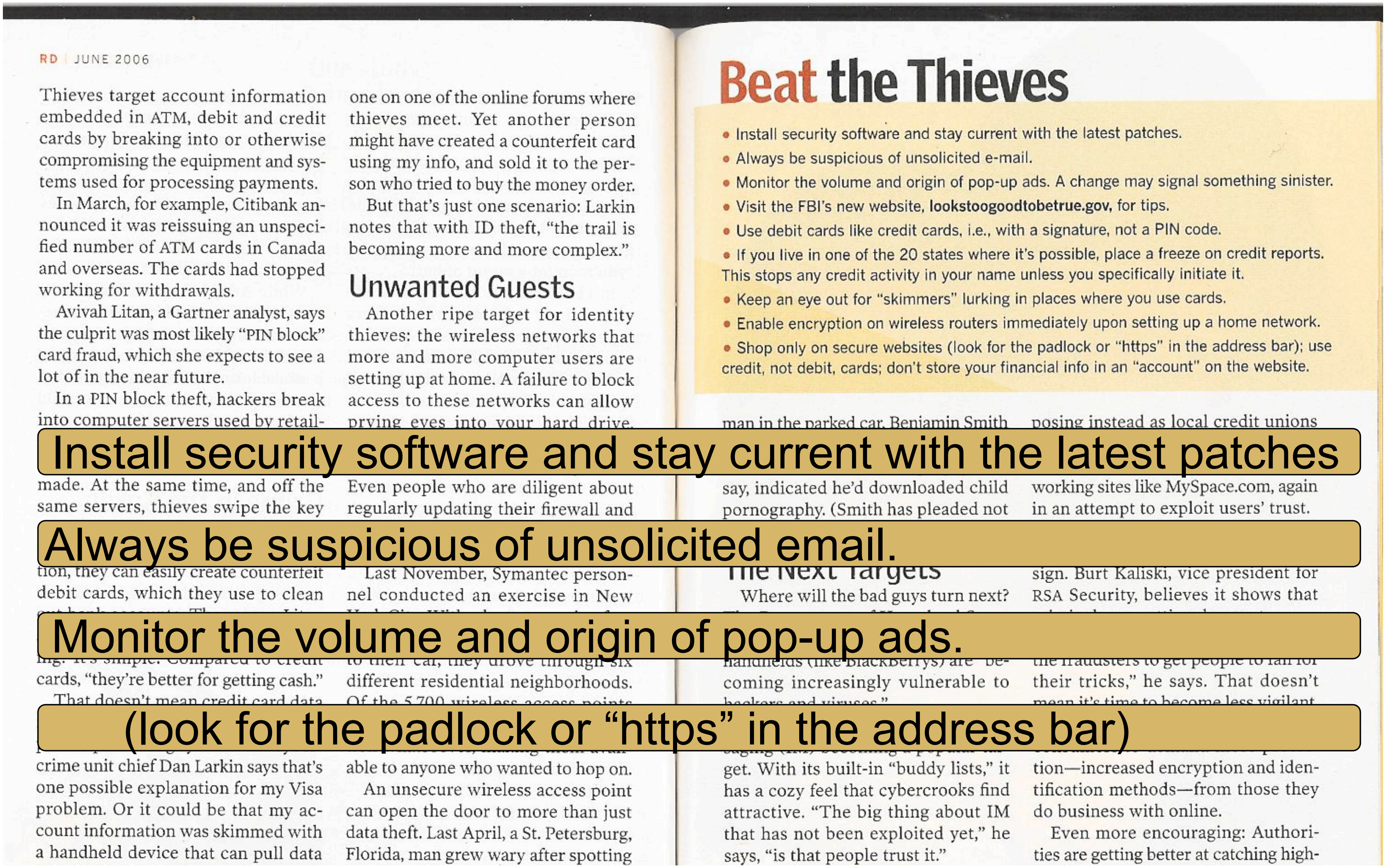
Why do we need Internet security education?

Airplane with all security features that will ever exist



Pilot who can be tricked that down is up

Traditional Education



RD | JUNE 2006

Thieves target account information embedded in ATM, debit and credit cards by breaking into or otherwise compromising the equipment and systems used for processing payments.

In March, for example, Citibank announced it was reissuing an unspecified number of ATM cards in Canada and overseas. The cards had stopped working for withdrawals.

Avivah Litan, a Gartner analyst, says the culprit was most likely "PIN block" card fraud, which she expects to see a lot of in the near future.

In a PIN block theft, hackers break into computer servers used by retail-

made. At the same time, and off the same servers, thieves swipe the key

tion, they can easily create counterfeit debit cards, which they use to clean

ing. It's simple. Compared to credit cards, "they're better for getting cash."

That doesn't mean credit card data

crime unit chief Dan Larkin says that's one possible explanation for my Visa problem. Or it could be that my account information was skimmed with a handheld device that can pull data

one on one of the online forums where thieves meet. Yet another person might have created a counterfeit card using my info, and sold it to the person who tried to buy the money order.

But that's just one scenario: Larkin notes that with ID theft, "the trail is becoming more and more complex."

Unwanted Guests

Another ripe target for identity thieves: the wireless networks that more and more computer users are setting up at home. A failure to block access to these networks can allow prying eyes into your hard drive.

Even people who are diligent about regularly updating their firewall and

Last November, Symantec personnel conducted an exercise in New

to their car, they drove through six different residential neighborhoods. Of the 5,700 wireless access points

able to anyone who wanted to hop on.

An unsecure wireless access point can open the door to more than just data theft. Last April, a St. Petersburg, Florida, man grew wary after spotting

Beat the Thieves

- Install security software and stay current with the latest patches.
- Always be suspicious of unsolicited e-mail.
- Monitor the volume and origin of pop-up ads. A change may signal something sinister.
- Visit the FBI's new website, **lookstoogoodtobetrue.gov**, for tips.
- Use debit cards like credit cards, i.e., with a signature, not a PIN code.
- If you live in one of the 20 states where it's possible, place a freeze on credit reports. This stops any credit activity in your name unless you specifically initiate it.
- Keep an eye out for "skimmers" lurking in places where you use cards.
- Enable encryption on wireless routers immediately upon setting up a home network.
- Shop only on secure websites (look for the padlock or "https" in the address bar); use credit, not debit, cards; don't store your financial info in an "account" on the website.

man in the parked car. Benjamin Smith

say, indicated he'd downloaded child pornography. (Smith has pleaded not

The Next Targets

Where will the bad guys turn next?

handhelds (like BlackBerrys) are becoming increasingly vulnerable to hackers and viruses."

get. With its built-in "buddy lists," it has a cozy feel that cybercrooks find attractive. "The big thing about IM that has not been exploited yet," he says, "is that people trust it."

posing instead as local credit unions

working sites like MySpace.com, again in an attempt to exploit users' trust.

sign. Burt Kaliski, vice president for RSA Security, believes it shows that

the fraudsters to get people to fall for their tricks," he says. That doesn't mean it's time to become less vigilant

tion—increased encryption and identification methods—from those they do business with online.

Even more encouraging: Authorities are getting better at catching high-

Install security software and stay current with the latest patches

Always be suspicious of unsolicited email.

Monitor the volume and origin of pop-up ads.

(look for the padlock or "https" in the address bar)

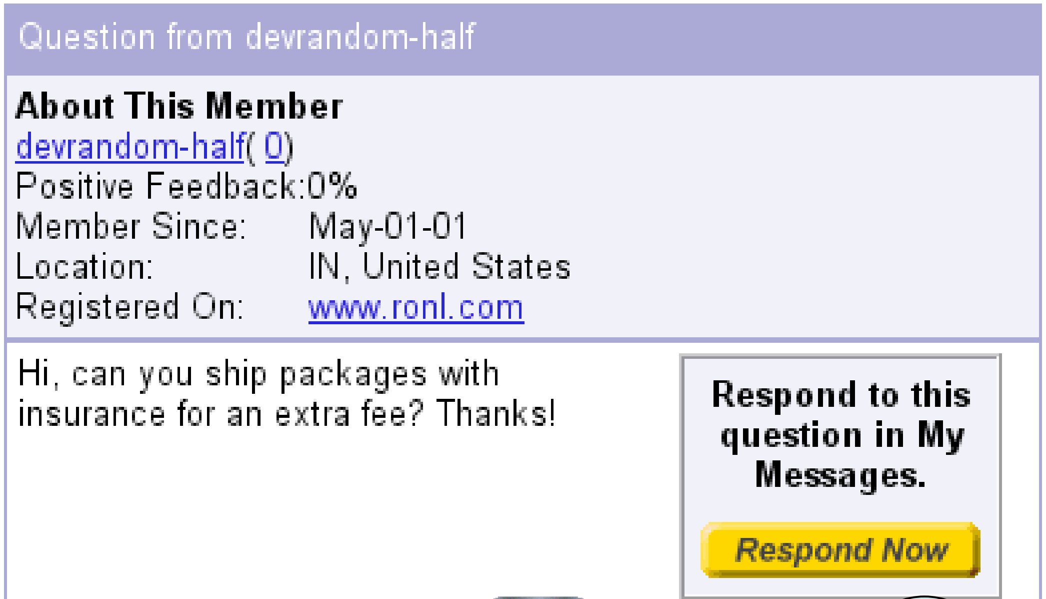
Why do we need phishing experiments?

To predict trends, knowing what the yet not exploited human vulnerabilities are.

Ethical and accurate assessments

With Ratkiewicz "Designing Ethical Phishing Experiments:
A study of (ROT13) rOnl auction query features" (WWW, 2006)

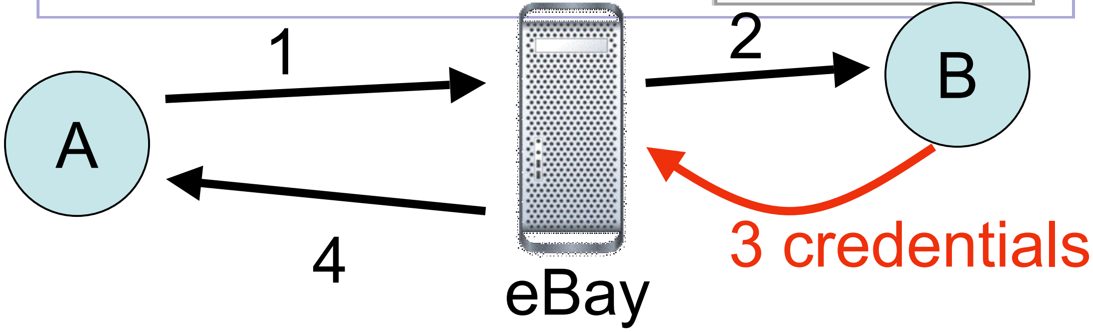
Reality:



Question from devrandom-half

About This Member
devrandom-half(0)
Positive Feedback:0%
Member Since: May-01-01
Location: IN, United States
Registered On: www.ronl.com

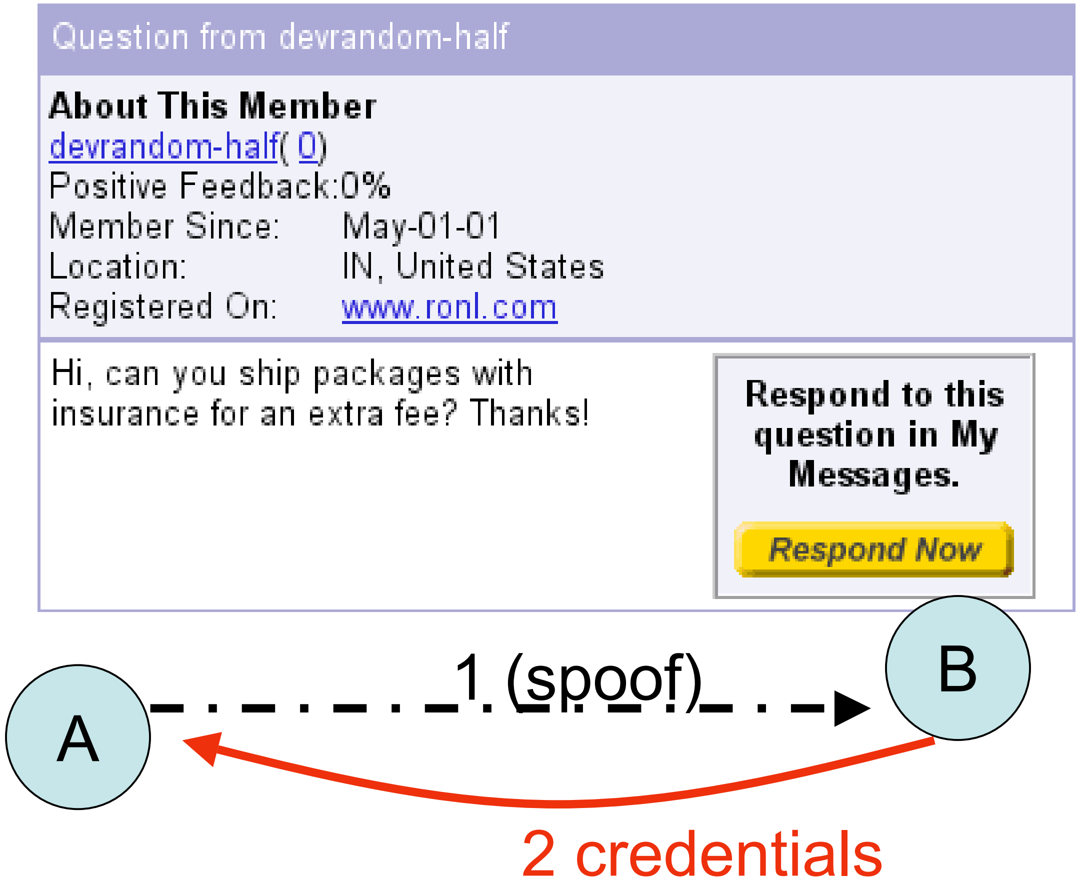
Hi, can you ship packages with insurance for an extra fee? Thanks!



Ethical and accurate assessments

With Ratkiewicz “Designing Ethical Phishing Experiments:
A study of (ROT13) rOnl auction query features” (WWW, 2006)

Attack:



Question from devrandom-half

About This Member
devrandom-half(0)
Positive Feedback:0%
Member Since: May-01-01
Location: IN, United States
Registered On: www.ronl.com

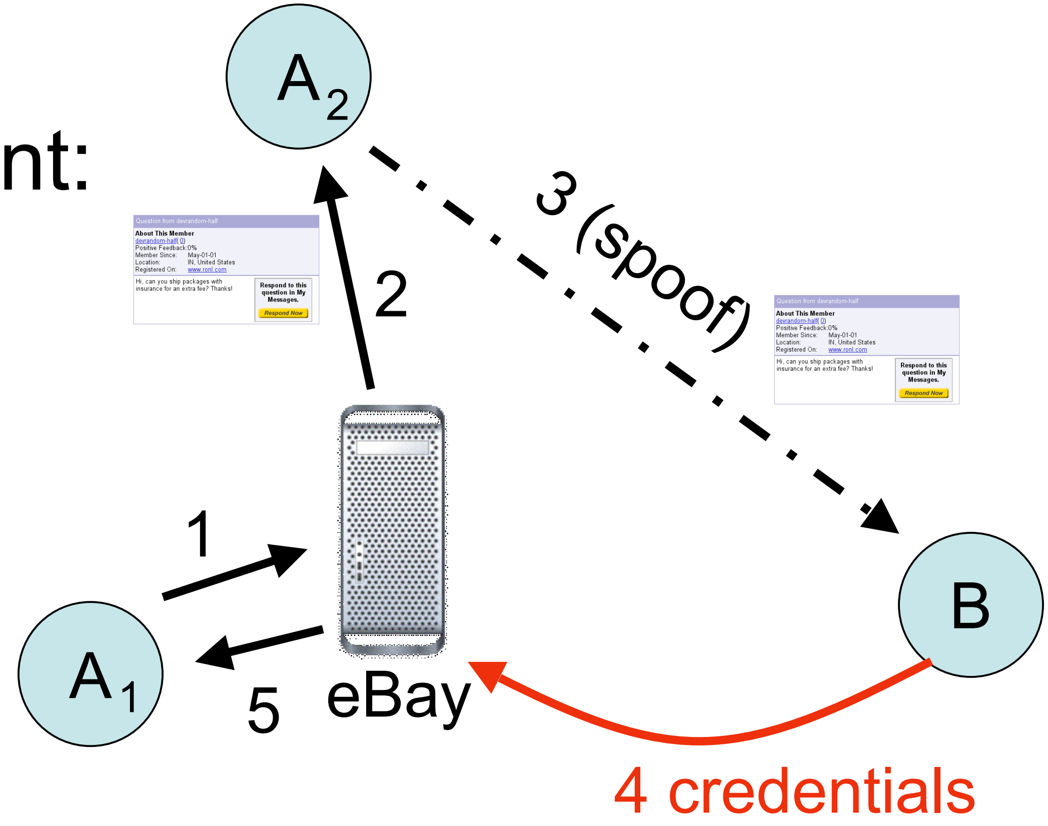
Hi, can you ship packages with insurance for an extra fee? Thanks!

Respond to this question in My Messages.

Ethical and accurate assessments

With Ratkiewicz “Designing Ethical Phishing Experiments:
A study of (ROT13) rOnl auction query features” (WWW, 2006)

Experiment:



Question from devrandom-half

About This Member
devrandom-half(0)
Positive Feedback:0%
Member Since: May-01-01
Location: IN, United States
Registered On: www.ronl.com

Hi, can you ship packages with insurance for an extra fee? Thanks!

Respond to this question in My Messages.

Question from devrandom-half

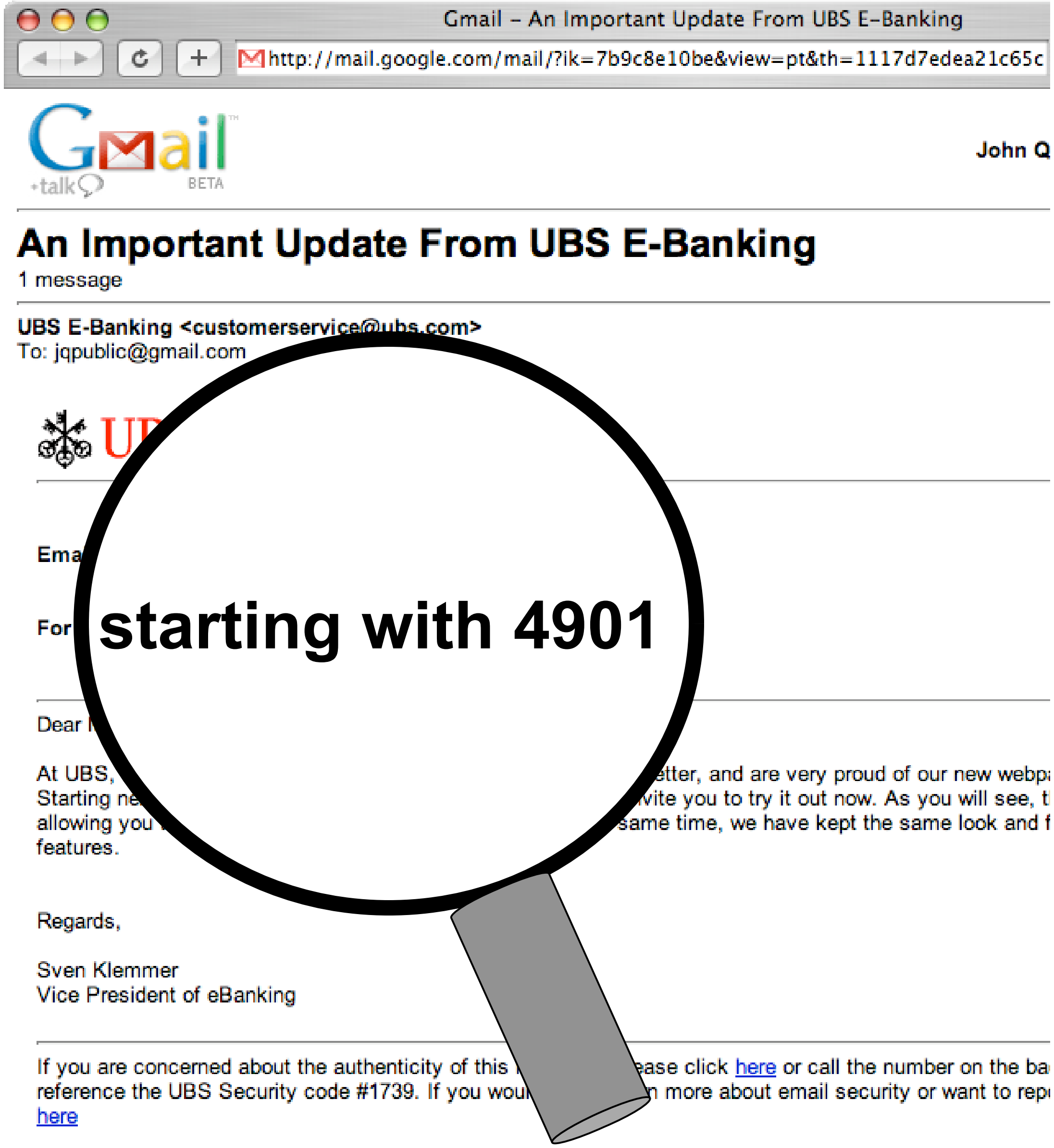
About This Member
devrandom-half(0)
Positive Feedback:0%
Member Since: May-01-01
Location: IN, United States
Registered On: www.ronl.com

Hi, can you ship packages with insurance for an extra fee? Thanks!

Respond to this question in My Messages.

Yield (incl spam filtering loss): 11% ± 3% …“eBay greeting” removed: same

Mutual authentication in the “real world”



Gmail – An Important Update From UBS E-Banking

http://mail.google.com/mail/?ik=7b9c8e10be&view=pt&th=1117d7edea21c65c

An Important Update From UBS E-Banking

1 message

UBS E-Banking <customerservice@ubs.com>
To: jqpublic@gmail.com

Ema

For

starting with 4901

Dear

At UBS, etter, and are very proud of our new webp
Starting ne vite you to try it out now. As you will see, t
allowing you same time, we have kept the same look and f
features.

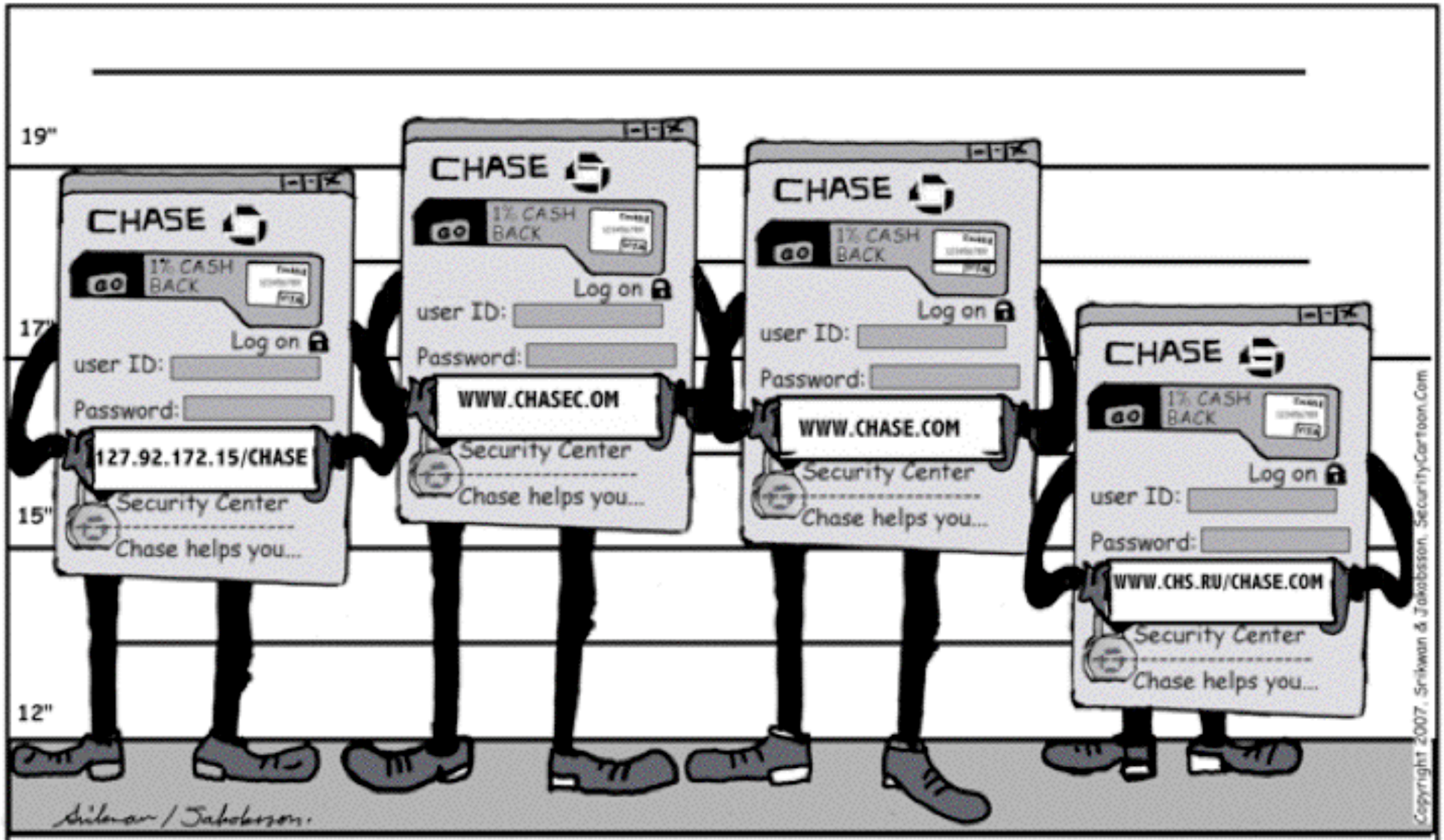
Regards,

Sven Klemmer
Vice President of eBanking

If you are concerned about the authenticity of this ease click here or call the number on the ba
reference the UBS Security code #1739. If you wou n more about email security or want to rep
here

With Tsow,Shah,Blevis,Lim, “What Instills Trust? A Qualitative Study of Phishing” (Abstract at Usable Security, 2007)

With Alex Tsow, “Deceit and Deception: A Large User Study of Phishing” (in submission)

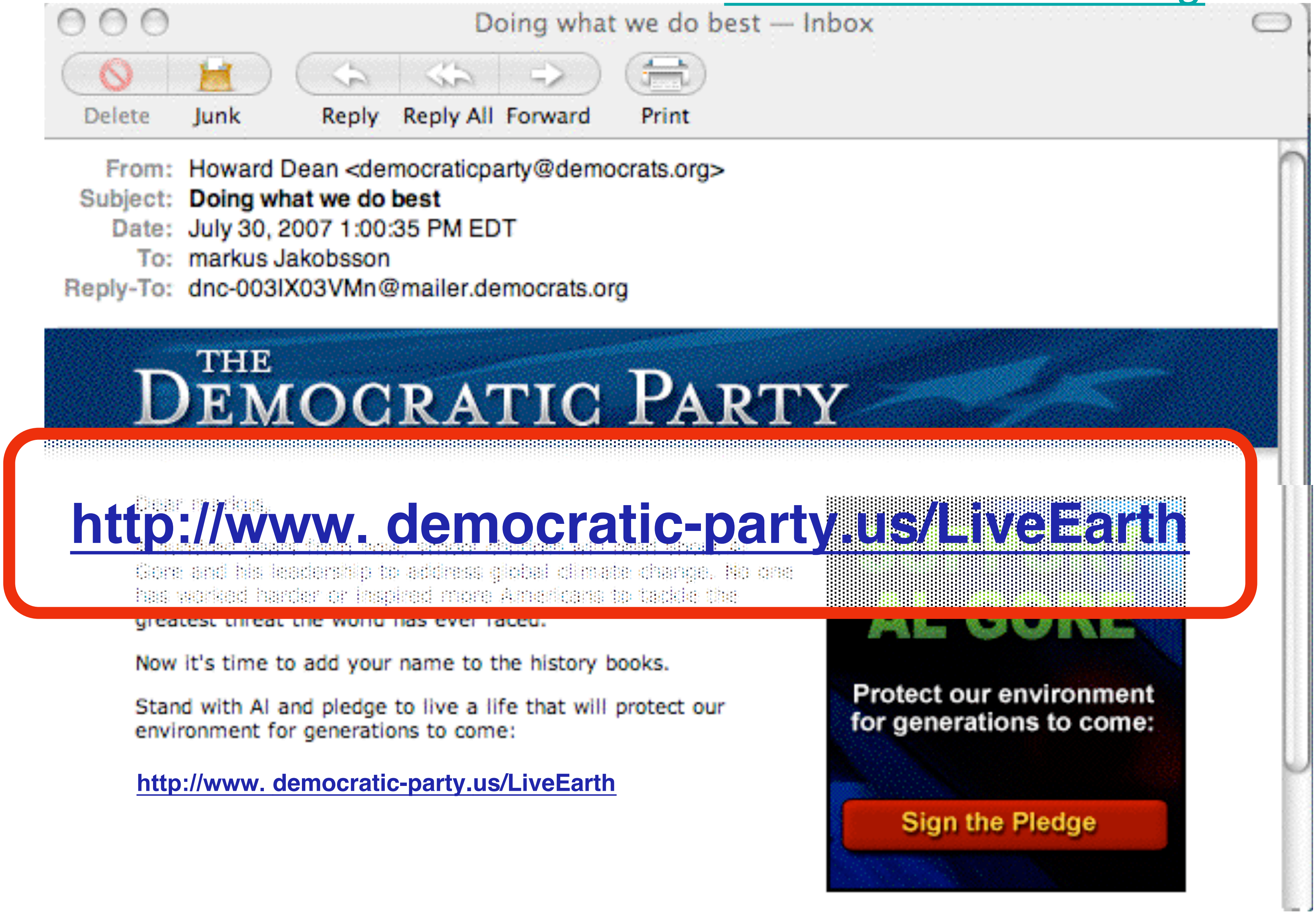


"SO, WHICH ONE WAS IT THAT ROBBED YOU?"

www.SecurityCartoon.com

And next? *Politishing?*

Annotated slides available at www.human-factor.org



From: Howard Dean <democraticparty@democrats.org>
Subject: **Doing what we do best**
Date: July 30, 2007 1:00:35 PM EDT
To: markus Jakobsson
Reply-To: dnc-003IX03VMn@mailer.democrats.org

THE DEMOCRATIC PARTY

http://www. democratic-party.us/LiveEarth

Dear markus,

Gore and his leadership to address global climate change. No one has worked harder or inspired more Americans to tackle the greatest threat the world has ever faced.

Now it's time to add your name to the history books.

Stand with Al and pledge to live a life that will protect our environment for generations to come:

http://www. democratic-party.us/LiveEarth