25 – User education and phishing

Lorrie Cranor, Blase Ur, and Rich Shay

April 14, 2015

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com] Sent: Sun 2/5/2006 6:03 PM

To: isri-people@cs.cmu.edu

Cc:

Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

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

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com] Sent: Sun 2/5/2006 6:03 PM

To: isri-people@cs.cmu.edu

eBay: Urgent Notification From Billing Department

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

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com] Sent: Sun 2/5/2006 6:03 PM

To: isri-people@cs.cmu.edu

Cc:

Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't update 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

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com] Sent: Sun 2/5/2006 6:03 PM

To: isri-people@cs.cmu.edu

Cc:

Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

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:

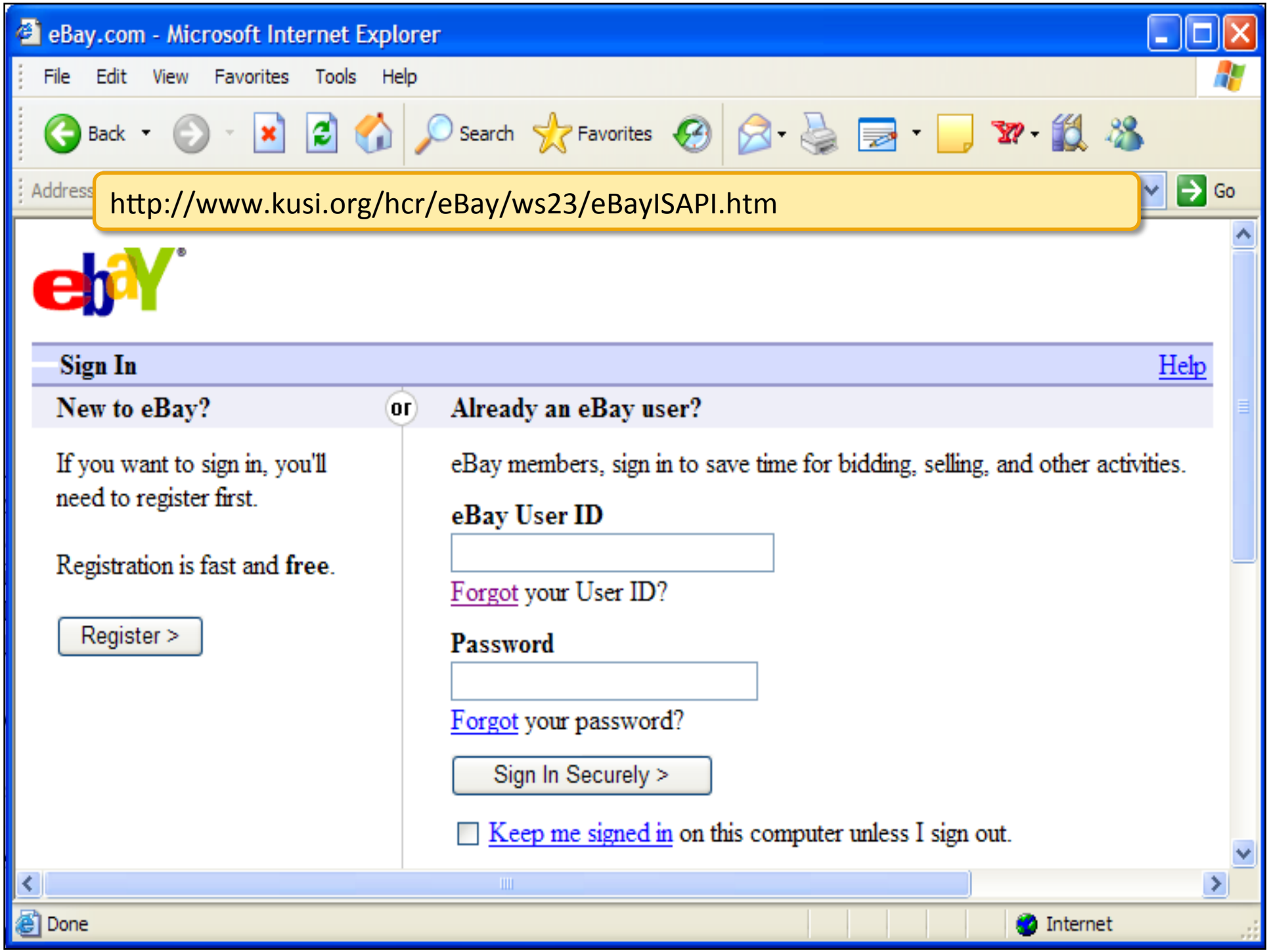
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&sidteid=0

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


eBay.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
http://www.kusi.org/hcr/eBay/ws23/eBayISAPI.htm
Go
Sign In
Help
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
eBay members, sign in to save time for bidding, selling, and other activities.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Sign In Securely >
Keep me signed in on this computer unless I sign out.
Done
Internet

Phishing works

- 73 million US adults received more than 50 phishing emails each in the year 2005
- Gartner estimated 3.6 million adults lost $3.2 billion in phishing attacks in 2007
- Financial institutions and military are also victims
- Corporate espionage

Why phishing works

- Phishers take advantage of Internet users' trust in legitimate organizations
- Lack of computer and security knowledge [Dhamija et al.]
- People don't use good strategies to protect themselves [Downs et al.]

Anti-phishing strategies

- Silently eliminate the threat
  - Find and take down phishing web sites
  - Detect and delete phishing emails
- Warn users about the threat
  - Anti-phishing toolbars and web browser features
- Train users not to fall for attacks

User education is challenging

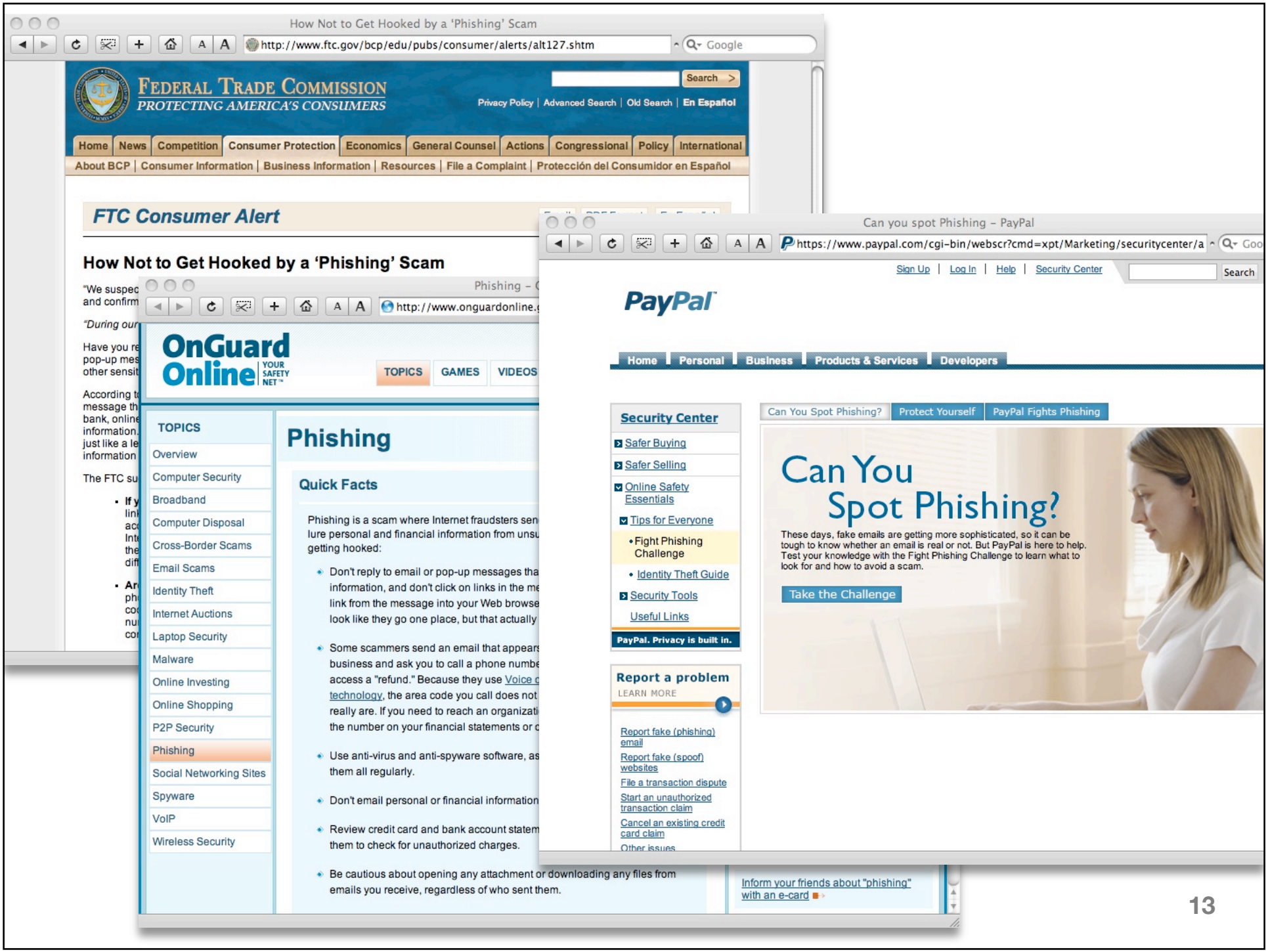
- Users are not motivated to learn about security
- For most users, security is a secondary task
- It is difficult to teach people to make the right online trust decision without increasing their false positive errors

Is user education possible?

- Security education "puts the burden on the wrong shoulder."
  [Nielsen, J. 2004. User education is not the answer to security problems. http://www.useit.com/alertbox/20041025.html.]

- "Security user education is a myth."
  [Gorling, S. 2006. The myth of user education. 16th Virus Bulletin International Conference.]

- "User education is a complete waste of time. It is about as much use as nailing jelly to a wall…. They are not interested…they just want to do their job."
  [Martin Overton, a U.K.-based security specialist at IBM, quoted in http://news.cnet.com/2100-7350_3-6125213-2.html]


How Not to Get Hooked by a 'Phishing' Scam
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Search
Privacy Policy | Advanced Search | Old Search | En Español
Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions | Congressional | Policy | International
About BCP | Consumer Information | Business Information | Resources | File a Complaint | Protección del Consumidor en Español
FTC Consumer Alert
How Not to Get Hooked by a 'Phishing' Scam
Can you spot Phishing - PayPal
https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/a
Sign Up | Log In | Help | Security Center
Search
PayPal
Home | Personal | Business | Products & Services | Developers
Security Center
Safer Buying
Safer Selling
Online Safety Essentials
Tips for Everyone
Fight Phishing Challenge
Identity Theft Guide
Security Tools
Useful Links
PayPal. Privacy is built in.
Report a problem
LEARN MORE
Report fake (phishing) email
Report fake (spoof) websites
File a transaction dispute
Start an unauthorized transaction claim
Cancel an existing credit card claim
Other issues
Can You Spot Phishing?
Protect Yourself
PayPal Fights Phishing
Can You Spot Phishing?
These days, fake emails are getting more sophisticated, so it can be tough to know whether an email is real or not. But PayPal is here to help. Test your knowledge with the Fight Phishing Challenge to learn what to look for and how to avoid a scam.
Take the Challenge
Phishing
OnGuard Online
YOUR SAFETY NET
TOPICS
GAMES
VIDEOS
TOPICS
Overview
Computer Security
Broadband
Computer Disposal
Cross-Border Scams
Email Scams
Identity Theft
Internet Auctions
Laptop Security
Malware
Online Investing
Online Shopping
P2P Security
Phishing
Social Networking Sites
Spyware
VoIP
Wireless Security
Quick Facts
Phishing is a scam where Internet fraudsters sen
lure personal and financial information from unsu
getting hooked:
Don't reply to email or pop-up messages tha
information, and don't click on links in the me
link from the message into your Web browse
look like they go one place, but that actually
Some scammers send an email that appears
business and ask you to call a phone numbe
access a "refund." Because they use Voice
technology, the area code you call does not
really are. If you need to reach an organizati
the number on your financial statements or
Use anti-virus and anti-spyware software, as
them all regularly.
Don't email personal or financial information
Review credit card and bank account statem
them to check for unauthorized charges.
Be cautious about opening any attachment or downloading any files from
emails you receive, regardless of who sent them.
Inform your friends about "phishing" with an e-card

Web site training study

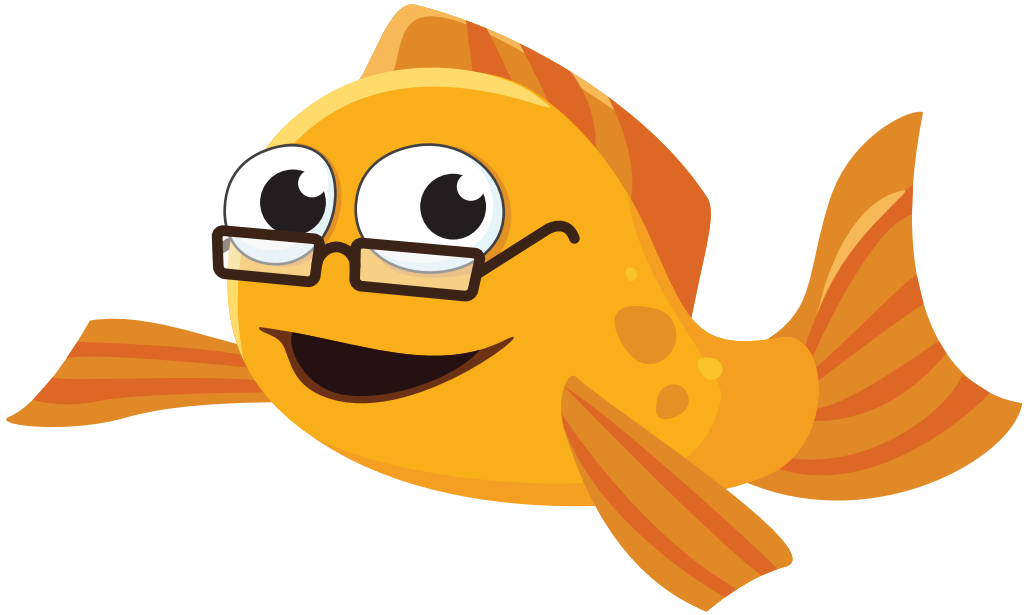
- Laboratory study of 28 non-expert computer users
- Control group: evaluate 10 sites, 15 minute break to read email or play solitaire, evaluate 10 more sites
- Experimental group: evaluate 10 sites, 15 minutes to read web-based training materials, evaluate 10 more sites
- Experimental group performed significantly better identifying phish after training, but more false positives
- People can learn from web-based training materials, if only we could get them to read them!

P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology (TOIT)*, Volume 10, Issue 2, May 2010.

How do we get people trained?

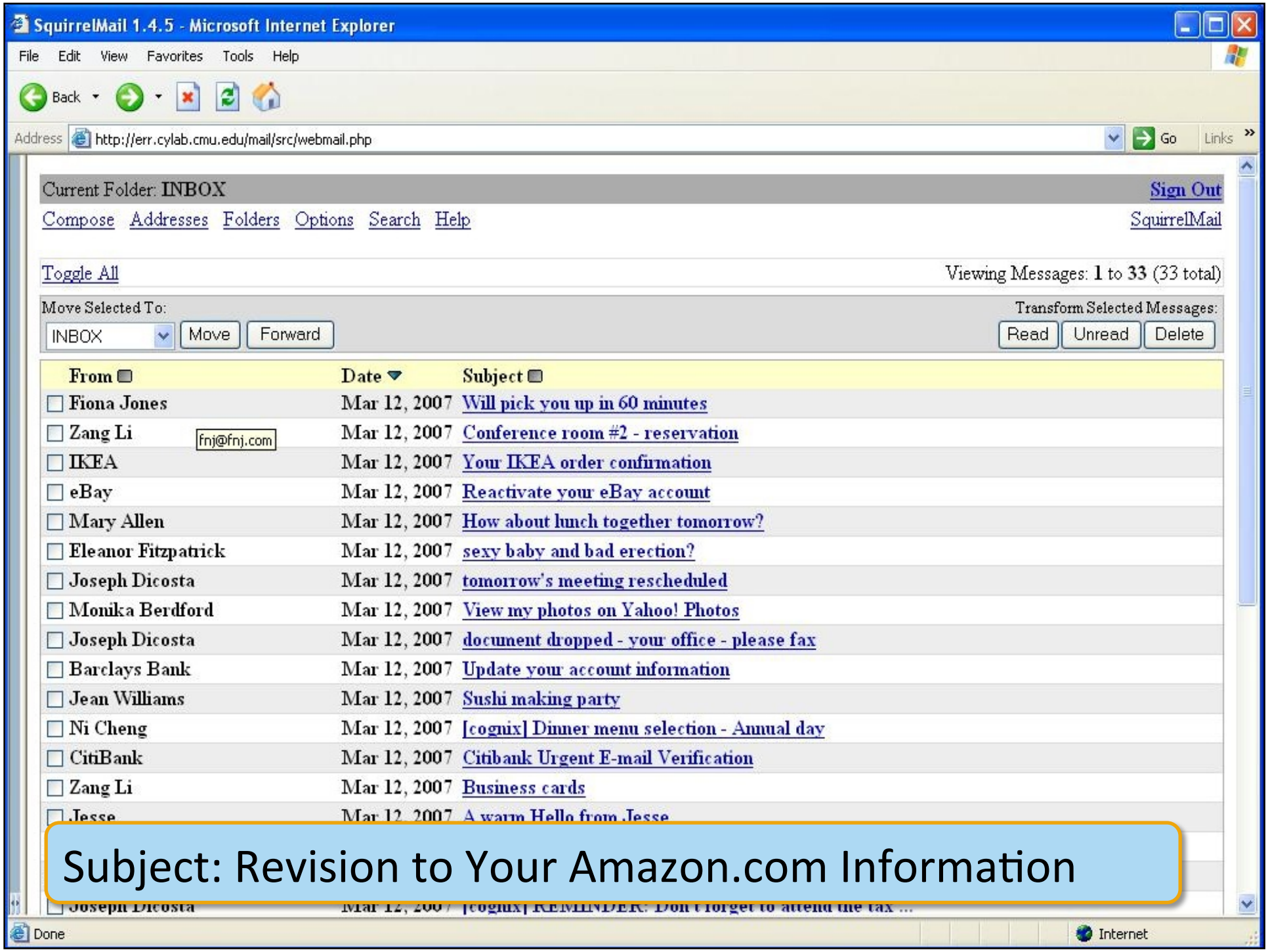
- Problem
  - Existing materials good, but could be better
  - Most people don't proactively look for security training materials
  - "Security notice" emails sent to employees and/or customers tend to be ignored
    - Too much to read
    - People don't consider them relevant
- Solution
  - Find a "teachable moment": PhishGuru
  - Make training fun: Anti-Phishing Phil
  - Use learning science principles

PhishGuru



PhishGuru Embedded training

- Send emails that looks like a phishing attack
- If recipient falls for it, intervention warns and highlights what cues to look for in succinct and engaging format
- User studies have demonstrated that this is effective
- Delivering same training via direct email is not effective!


SquirrelMail 1.4.5 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://err.cylab.cmu.edu/mail/src/webmail.php
Go
Links
Current Folder: INBOX
Sign Out
Compose Addresses Folders Options Search Help
SquirrelMail
Toggle All
Viewing Messages: 1 to 33 (33 total)
Move Selected To:
INBOX
Move
Forward
Transform Selected Messages:
Read
Unread
Delete
From
Date
Subject
Fiona Jones Mar 12, 2007 Will pick you up in 60 minutes
Zang Li fnj@fnj.com Mar 12, 2007 Conference room #2 - reservation
IKEA Mar 12, 2007 Your IKEA order confirmation
eBay Mar 12, 2007 Reactivate your eBay account
Mary Allen Mar 12, 2007 How about lunch together tomorrow?
Eleanor Fitzpatrick Mar 12, 2007 sexy baby and bad erection?
Joseph Dicosta Mar 12, 2007 tomorrow's meeting rescheduled
Monika Berdford Mar 12, 2007 View my photos on Yahoo! Photos
Joseph Dicosta Mar 12, 2007 document dropped - your office - please fax
Barclays Bank Mar 12, 2007 Update your account information
Jean Williams Mar 12, 2007 Sushi making party
Ni Cheng Mar 12, 2007 [cognix] Dinner menu selection - Annual day
CitiBank Mar 12, 2007 Citibank Urgent E-mail Verification
Zang Li Mar 12, 2007 Business cards
Jesse Mar 12, 2007 A warm Hello from Jesse
Subject: Revision to Your Amazon.com Information
Done
Internet

Message List | Delete Previous | Next Forward | Forward as Attachment | Reply | Reply All

Subject: Revision to Your Amazon.com Information
From: "Amazon" <service@amazon.com>
Date: Mon, March 12, 2007 4:15 pm
To: bsmith@cognix.com
Priority: Normal

Subject: Revision to Your Amazon.com Information

amazon.com.

Please login and enter your information

ssible

Please follow this link to update your personal information:

http://www.amazon.com/exec/obidos/sign-in.html

(To complete the verification process you must fill in all the required fields)

Please note: If you don't update your information within next 48 hours , we will be forced to suspend your account untill you have the time to contact us by phone.

We apreciate your support and understanding, as we work together to keep amazon market a safe place to trade. Thank you for your attention on this serious matter and we apologize.

Done Internet

Carnegie Mellon

The PhishGuru

Protect yourself from Phishing Scams

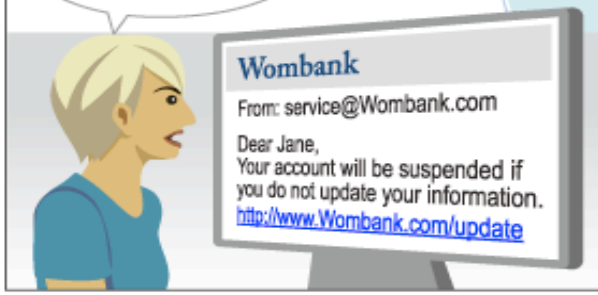
WARNING!

Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

How you were tricked

This email is from my bank and it is asking me to update my information. I better click on the link and update it.

STOP!
Don't fall for this scam email.



How to help protect yourself

1. Don't trust links in an email.

   http://www.amazon.com/update DANGER

2. Never give out personal information upon email request.

   Name: Jane Smith
   SSN: 123 DANGER 6789

3. Look carefully at the web address.

   http://www.annan.com

4. Type in the real website address into a web browser.

   http://www.amazon.com

5. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

   Credit Card Statement
   For customer service call 1-800-xxx-xxxx

6. Don't open unexpected email attachments or instant message download links.

   My Inbox
   Here is the updated document.
   attachment

How phishers trick you

Here is how con artists try to steal your personal information.

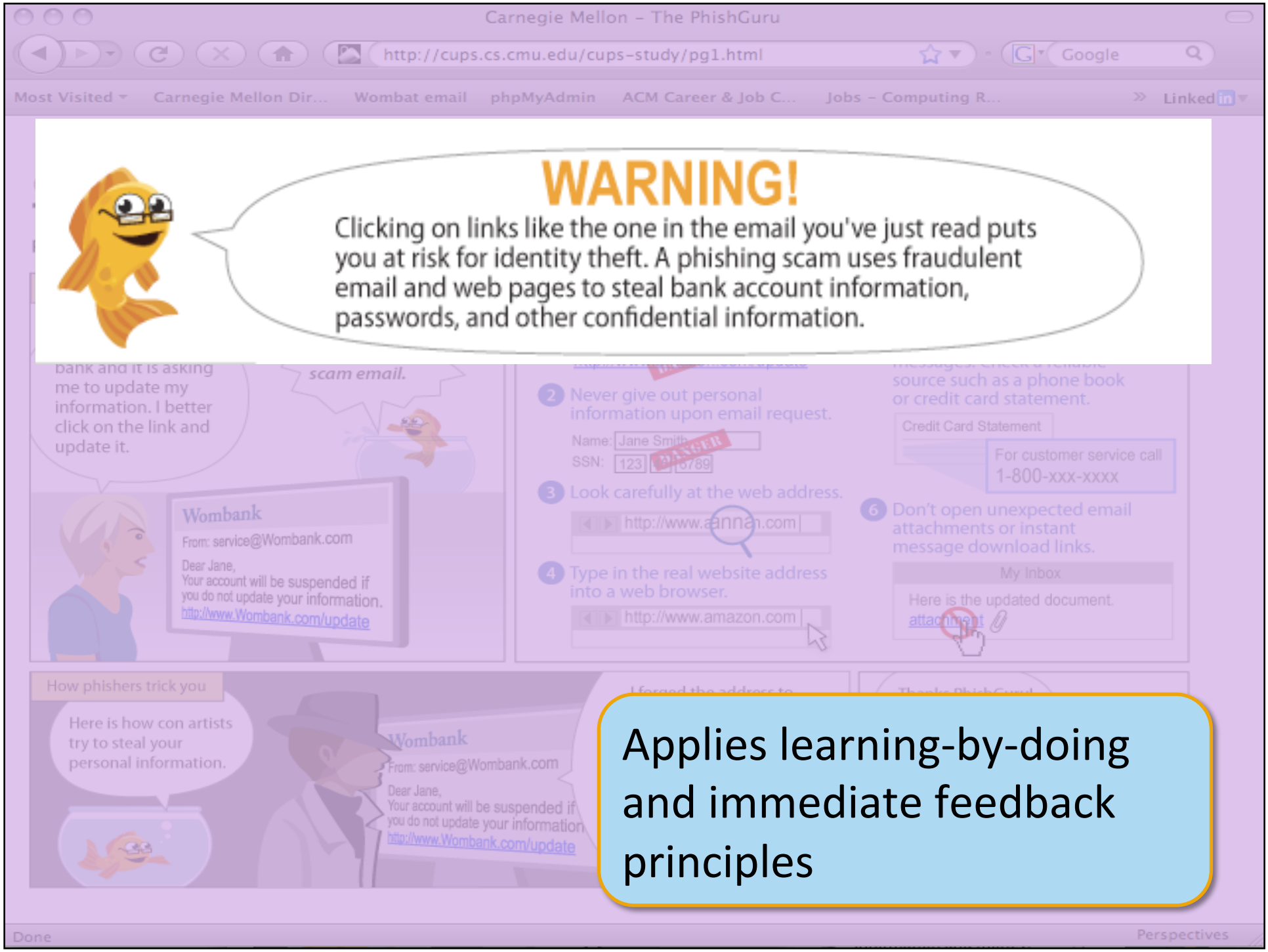
I forged the address to look genuine.

I threatened the user with an urgent message.

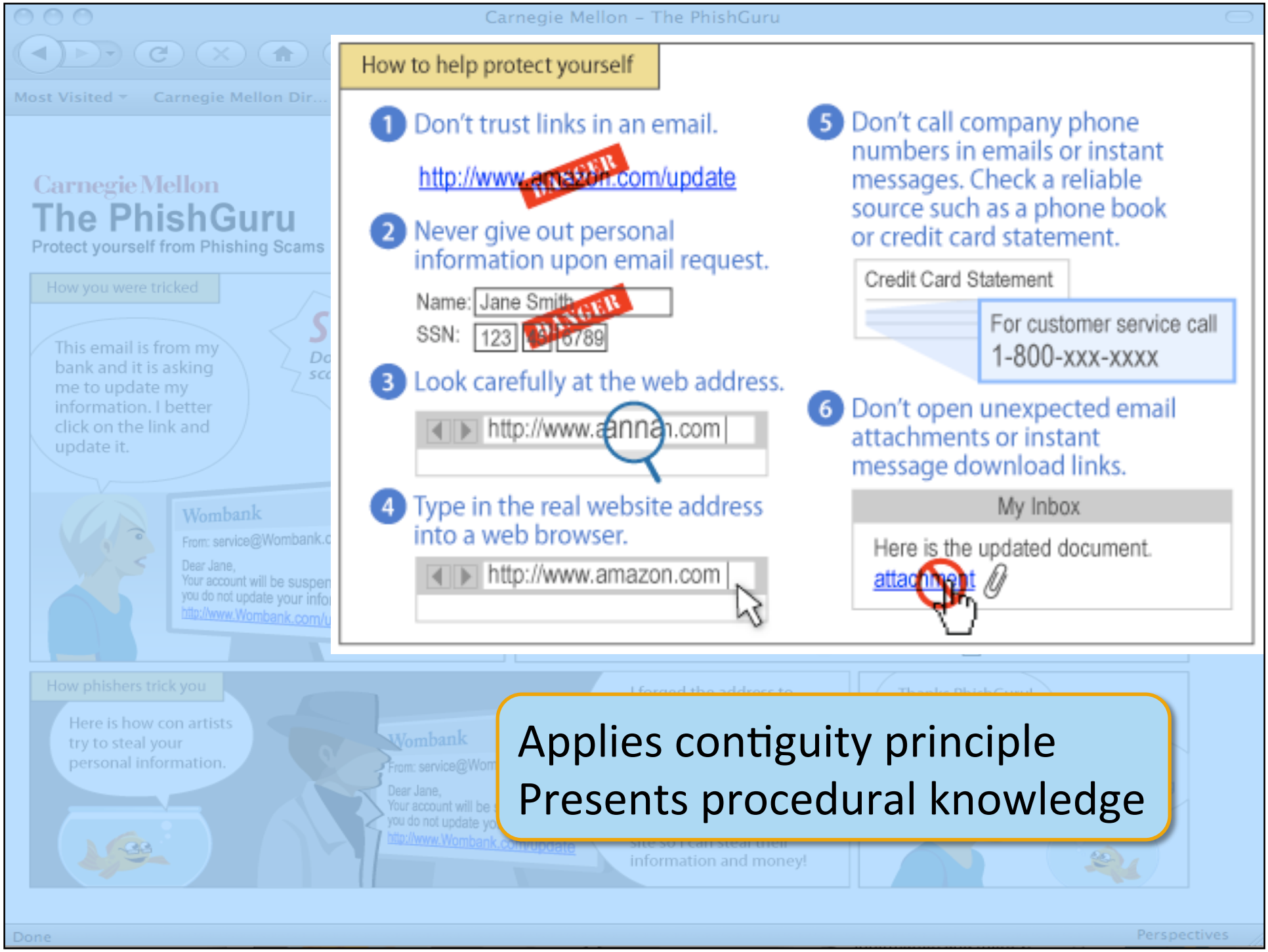
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!

Thanks PhishGuru! Where can I learn more?

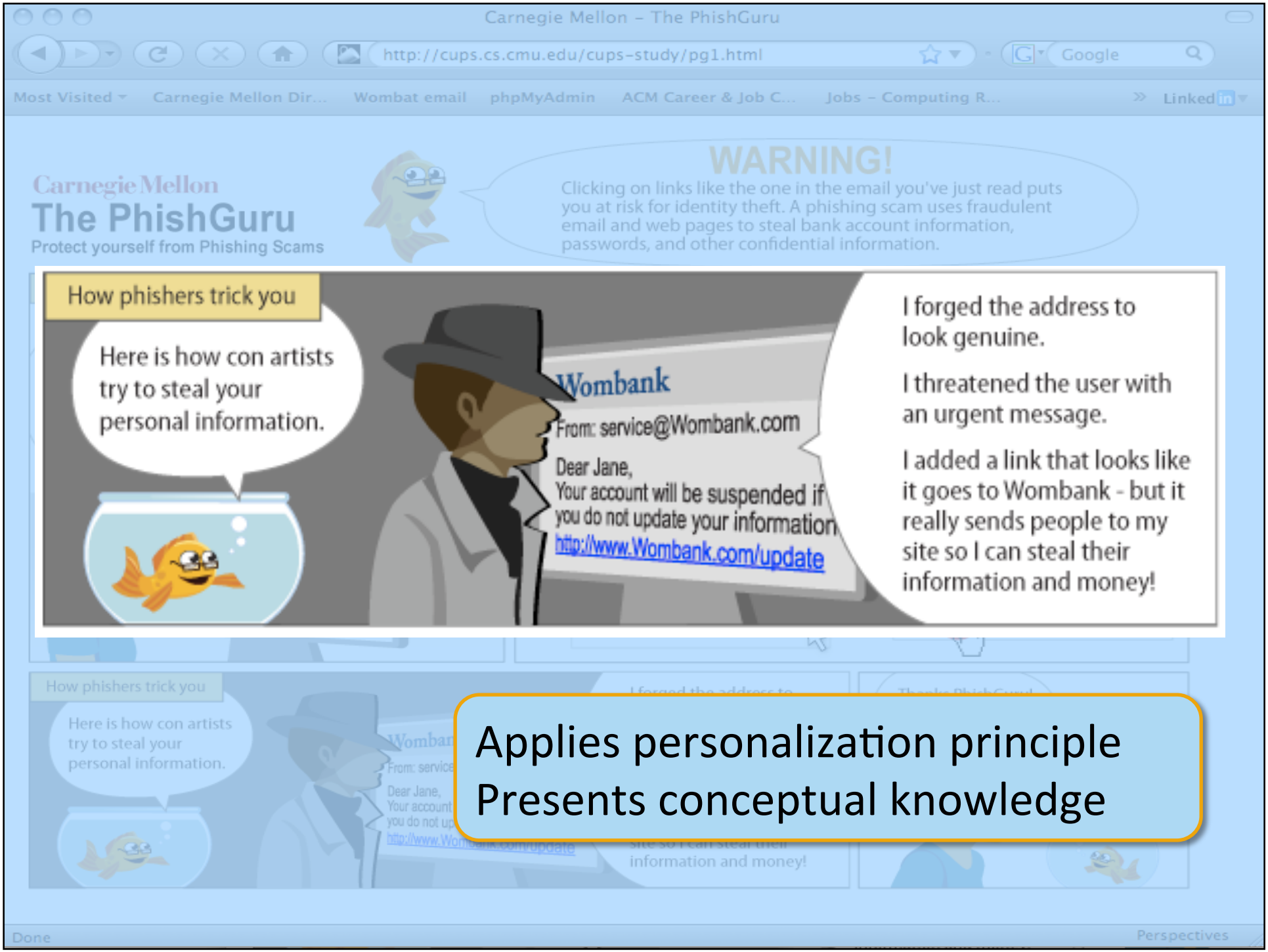
Visit phishguru.org


Carnegie Mellon – The PhishGuru
http://cups.cs.cmu.edu/cups-study/pg1.html
Google
Most Visited
Carnegie Mellon Dir...
Wombat email
phpMyAdmin
ACM Career & Job C...
Jobs – Computing R...
Linked
WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.
bank and it is asking me to update my information. I better click on the link and update it.
scam email.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
2 Never give out personal information upon email request.
Name: Jane Smith
SSN: 123 6789
DANGER
3 Look carefully at the web address.
http://www.aannan.com
4 Type in the real website address into a web browser.
http://www.amazon.com
source such as a phone book or credit card statement.
Credit Card Statement
For customer service call 1-800-xxx-xxxx
6 Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.
attachment
How phishers trick you
Here is how con artists try to steal your personal information.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information
http://www.Wombank.com/update
Applies learning-by-doing and immediate feedback principles
Done
Perspectives

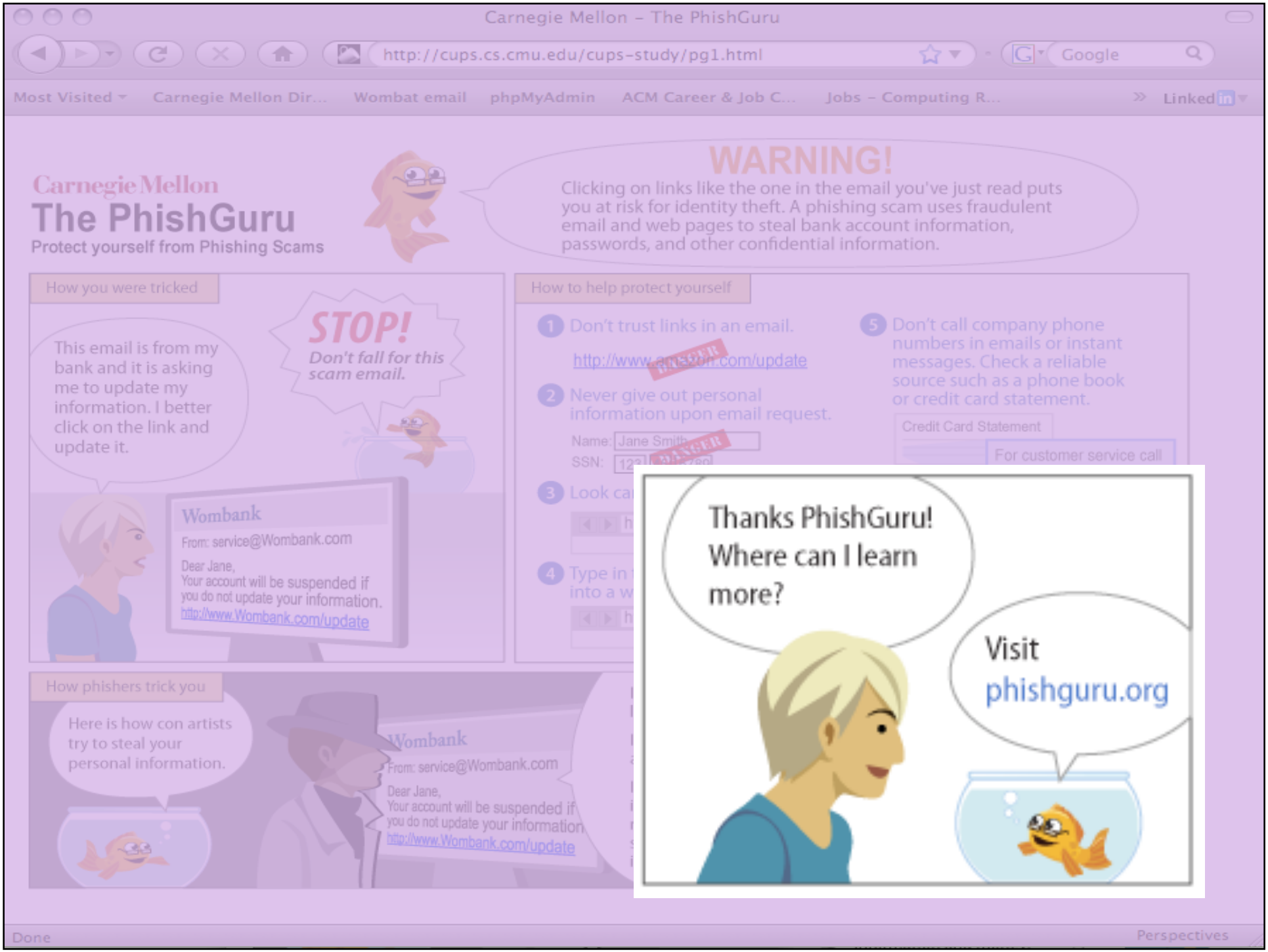
Applies story-based agent principle



Applies contiguity principle
Presents procedural knowledge



Applies personalization principle
Presents conceptual knowledge


Carnegie Mellon – The PhishGuru
http://cups.cs.cmu.edu/cups-study/pg1.html
Google
Most Visited
Carnegie Mellon Dir...
Wombat email
phpMyAdmin
ACM Career & Job C...
Jobs – Computing R...
Linked
Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams
WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.
How you were tricked
This email is from my bank and it is asking me to update my information. I better click on the link and update it.
STOP!
Don't fall for this scam email.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
How to help protect yourself
1 Don't trust links in an email.
2 Never give out personal information upon email request.
Name: Jane Smith
SSN:
5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For customer service call
How phishers trick you
Here is how con artists try to steal your personal information.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
Thanks PhishGuru! Where can I learn more?
Visit phishguru.org
Done
Perspectives

From research to reality

- Iterated on PhishGuru designs
- Phishguru user studies
  - Laboratory
  - Real-world
- Anti-Phishing Working Group landing page
- PhishGuru now being commercialized by Wombat Security Technologies, Inc.

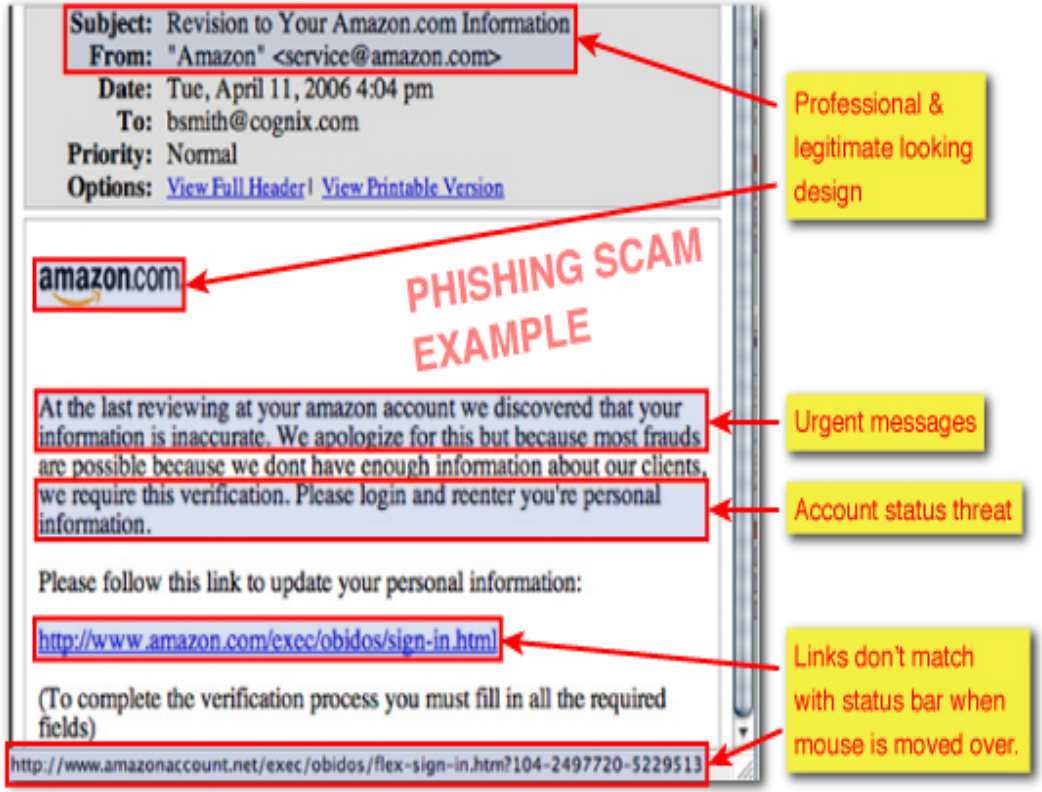
Protect yourself from Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**.
This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.

1. What's a phishing scam?

- Scammers send fake emails impersonating well-known companies to trick you into giving them your personal information.
- Giving up your personal information such as Social Security Number, credit card number, or account password will lead to identity theft and financial loss.

2. What does a phishing scam look like?



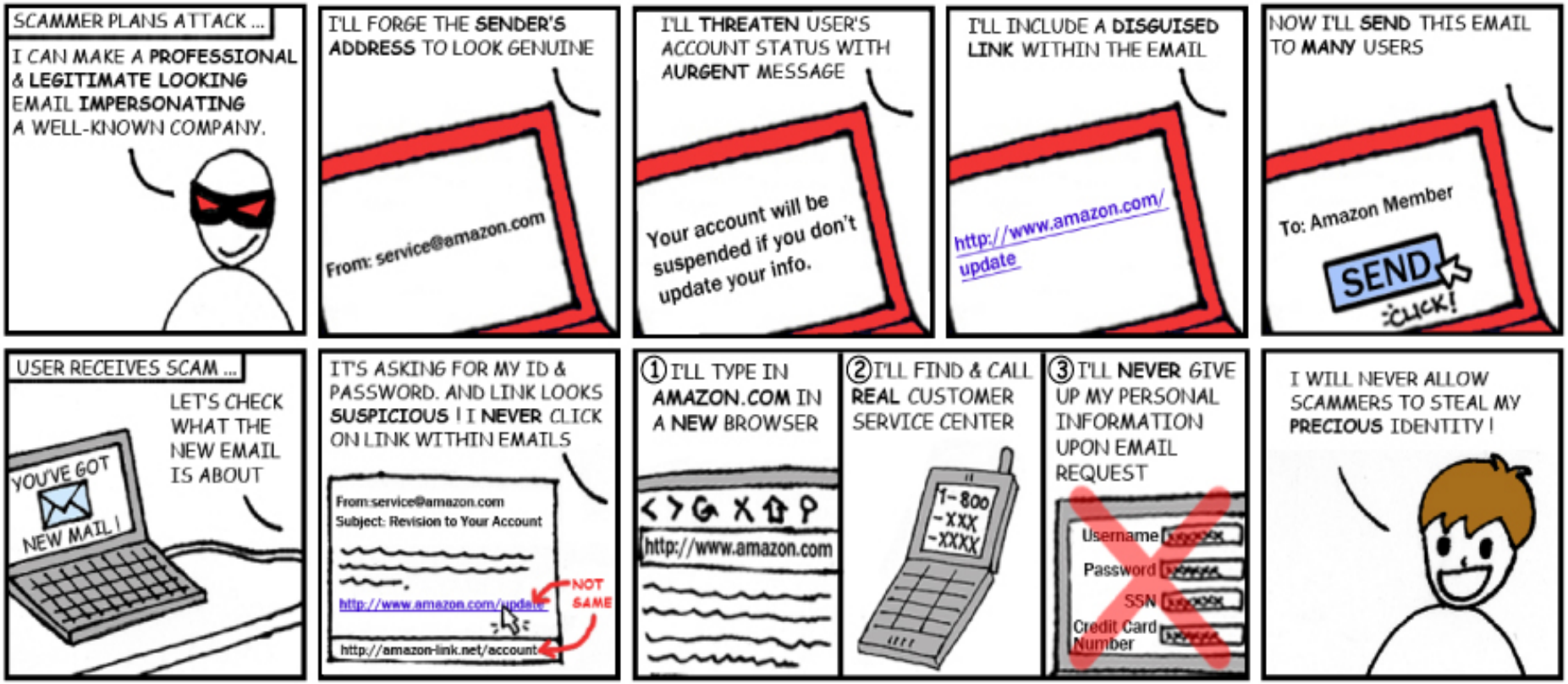
3. What are simple ways to protect yourself from phishing scams?

- **Never click on links within emails:** Never click on links within emails or reply to emails asking for your personal information.
- **Initiate contact:** Always access a website by typing in the real website address into the web browser.

- **Call customer service:** Never trust phone numbers within emails. Look it up yourself and call the customer service when email seems suspicious.
- **Never give out personal information:** Never give out personal information upon email request. Companies will rarely ask for your personal information via emails.

Protect Yourself from Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**.
This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.



The PhishGuru Protect yourself from Phishing Scams

Clicking on links like the one in the "amazon.com" email you've just read puts you at risk for identity theft and financial loss.

This email and tutorial were developed by Carnegie Mellon University to teach you how to protect yourself from these kind of phishing scams.

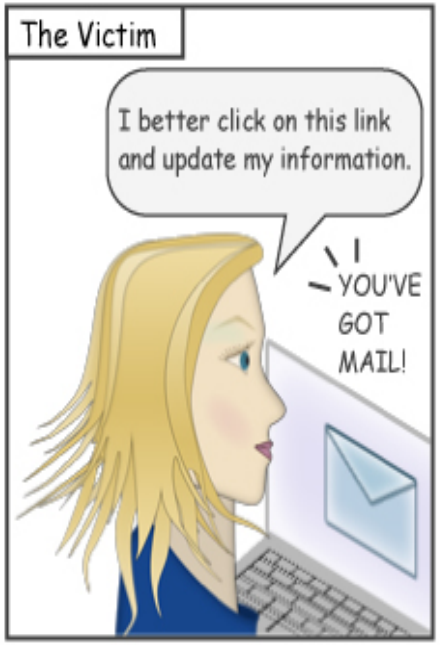
I forged the address to look genuine.

Then I threatened the user with an urgent message.

I added a link that looks like it goes to a book store, but really it sends people to my site so I can steal their information !

From: service@amazon.com
To: molly@mymail.com
amazon.com
Your account will be suspended if you do not update your account information.

http://www.amazon.com/update



STOP ! Follow these steps when reading your email:

1. Never click on links within emails.

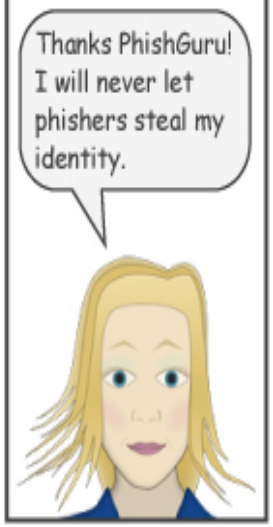
   http://www.amazon.com/update

2. Type in the real website address into a web browser.

3. Find and call a real customer service center.

4. Never give out personal information upon an email request.

5. Always be wary of suspicious websites.



Phishing

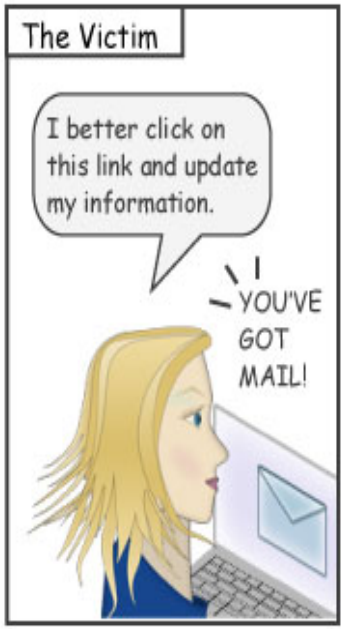
Clicking on links like the one in the email you've just read puts you at risk for identity theft and financial loss. Such emails are called phishing scams.

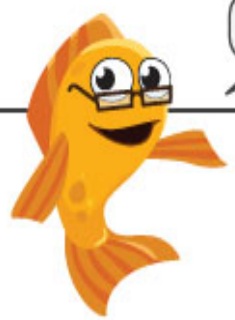
I **forged** the address to look **genuine**.

Then I **threatened** the user with an **urgent** message.

I added a link that looks like it goes to a book store, but really it sends people to my site so I can steal their information !

From: service@amazon.com
To: molly@mymail.com
amazon.com
Your account will be suspended if you do not update your account information.
http://www.amazon.com/update



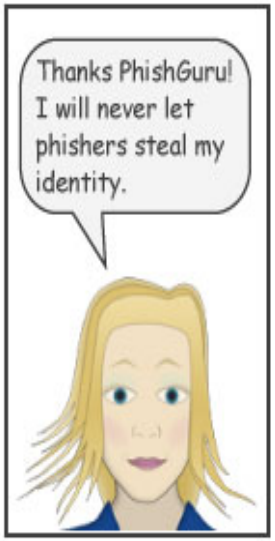


1. Never click on links within emails.
   http://www.amazon.com/update
2. Never give out personal information upon an email request.
   Username Molly
   Password **********
3. Find and call a real customer service center.

4. Type in the real website address into a web browser.

5. Always be wary of suspicious websites.

annazon.com



To learn more about protecting yourself from phishing scams and play an anti-phishing game visit http://phishguru.cs.cmu.edu.

Carnegie Mellon

The PhishGuru

Protect yourself from Phishing Scams

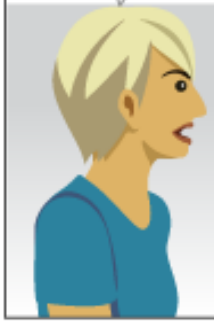
WARNING!

Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

How you were tricked

This email is from my bank and it is asking me to update my information. I better click on the link and update it.

STOP!
Don't fall for this scam email.



Wombank

From: service@Wombank.com

Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update

How to help protect yourself

1. Don't trust links in an email.

   http://www.amazon.com/update DANGER

2. Never give out personal information upon email request.

   Name: Jane Smith DANGER
   SSN: 123 [redacted] 6789

3. Look carefully at the web address.

   http://www.anna n.com

4. Type in the real website address into a web browser.

   http://www.amazon.com

5. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

   Credit Card Statement
   For customer service call 1-800-xxx-xxxx

6. Don't open unexpected email attachments or instant message download links.

   My Inbox
   Here is the updated document.
   attachment

How phishers trick you

Here is how con artists try to steal your personal information.

Wombank

From: service@Wombank.com

Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update

I forged the address to look genuine.

I threatened the user with an urgent message.

I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!

Thanks PhishGuru! Where can I learn more?

Visit phishguru.org

Carnegie Mellon

The PhishGuru

Protect yourself from Phishing Scams

WARNING!

Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

Follow these steps to protect yourself

1. Don't trust links in an email.

   http://www.amazon.com/update DANGER

2. Never give out personal information upon email request.

   Name: Jane Smith
   SSN: 123 [illegible] 6789 DANGER

3. Look carefully at the web address.

   http://www.aannan.com

4. Type in the real website address into a web browser.

   http://www.amazon.com

5. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

   Credit Card Statement
   For customer service call 1-800-xxx-xxxx

6. Don't open unexpected email attachments or instant message download links.

   My Inbox
   Here is the updated document.
   attachment

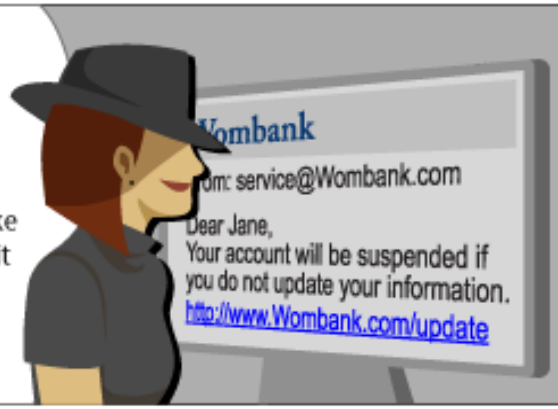
How phishers trick you

Here is how con artists try to steal your personal information.

I forged the address to look genuine.

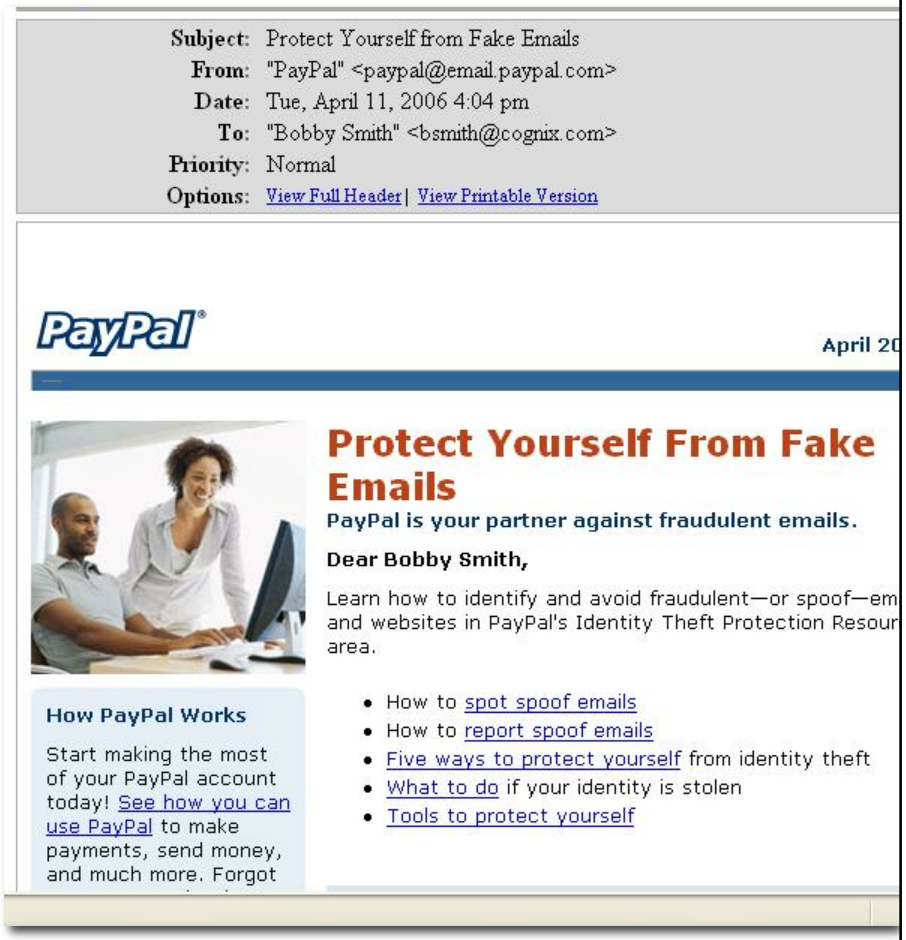
I threatened the user with an urgent message.

I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!



First lab study results

- Security notices are an ineffective medium for training users
- Users educated with embedded training make better decisions than those sent security notices



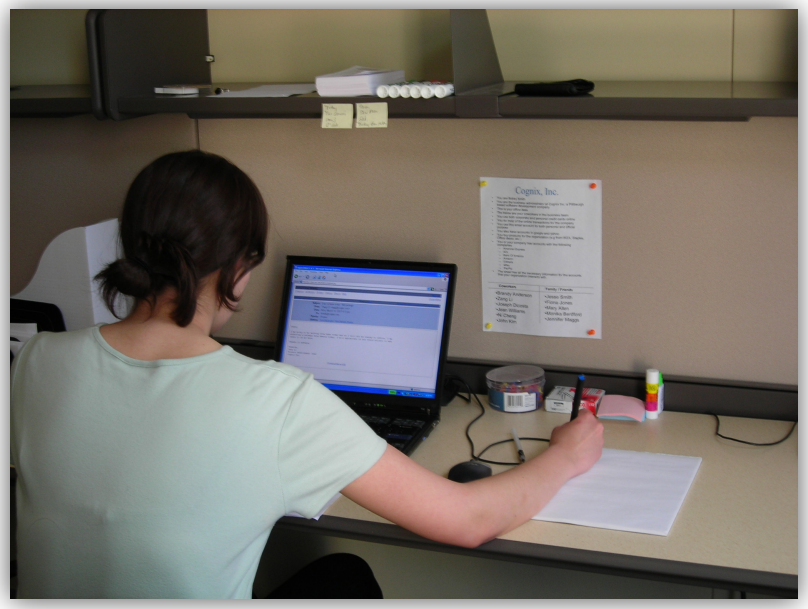
Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. Protecting people from phishing: the design and evaluation of an embedded training email system. CHI '07, pp. 905-914.

Goals for second lab study

- Investigate knowledge retention
- Investigate different delivery channels
  - Do people need to fall for phishing emails to get trained?

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., and Hong, J. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. e-Crime Researchers Summit, Anti-Phishing Working Group (2007).

Study design



- Setup
  - Think aloud study
  - Role play as Bobby Smith, business administrator
  - Respond to Bobby's email
- Experiment
  - Part 1: 33 emails and one intervention
  - Part 2 (after 7 days): 16 emails and no intervention
- 56 participants across 4 conditions
  - Control: no intervention
  - Suspicion: an email from a friend
  - Non-embedded: intervention in the email
  - Embedded: intervention after clicking on link

Some of Bobby's messages

Email type	Sender	Subject
Legitimate-no-link	Brandy Anderson	Booking hotel rooms for visitors
Legitimate-link	Joseph Dicosta	Please check PayPal balance
Phishing-no-account	Wells Fargo	Update your bank information!
Phishing-account	eBay	Reactivate your eBay account
Spam	Eddie Arredondo	Fw: Re: You will want this job
Intervention	Amazon	Revision to your Amazon.com information

Hypotheses

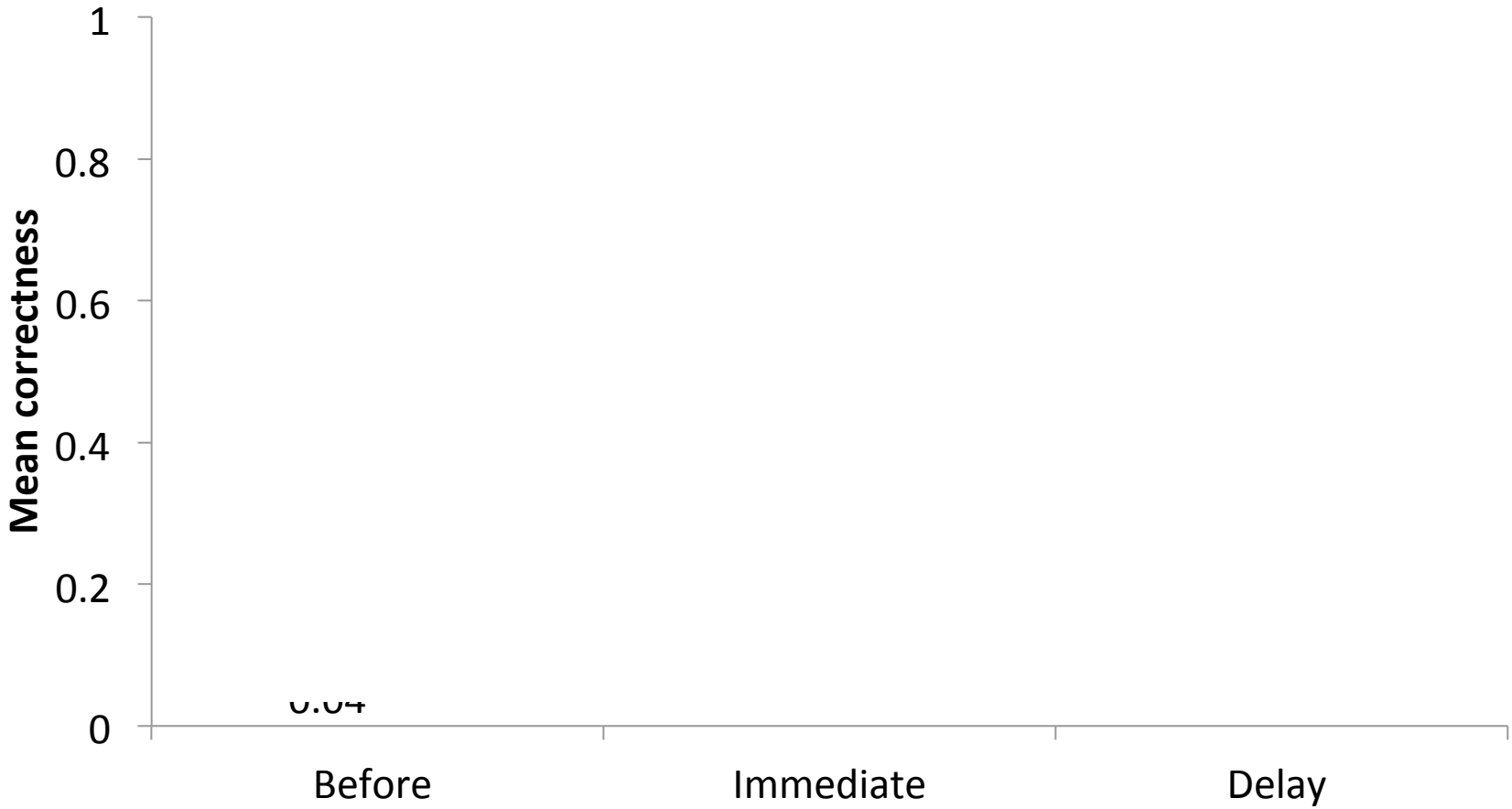
- Participants in embedded condition
  - Learn more effectively
  - Retain more knowledge

  than participants in other conditions

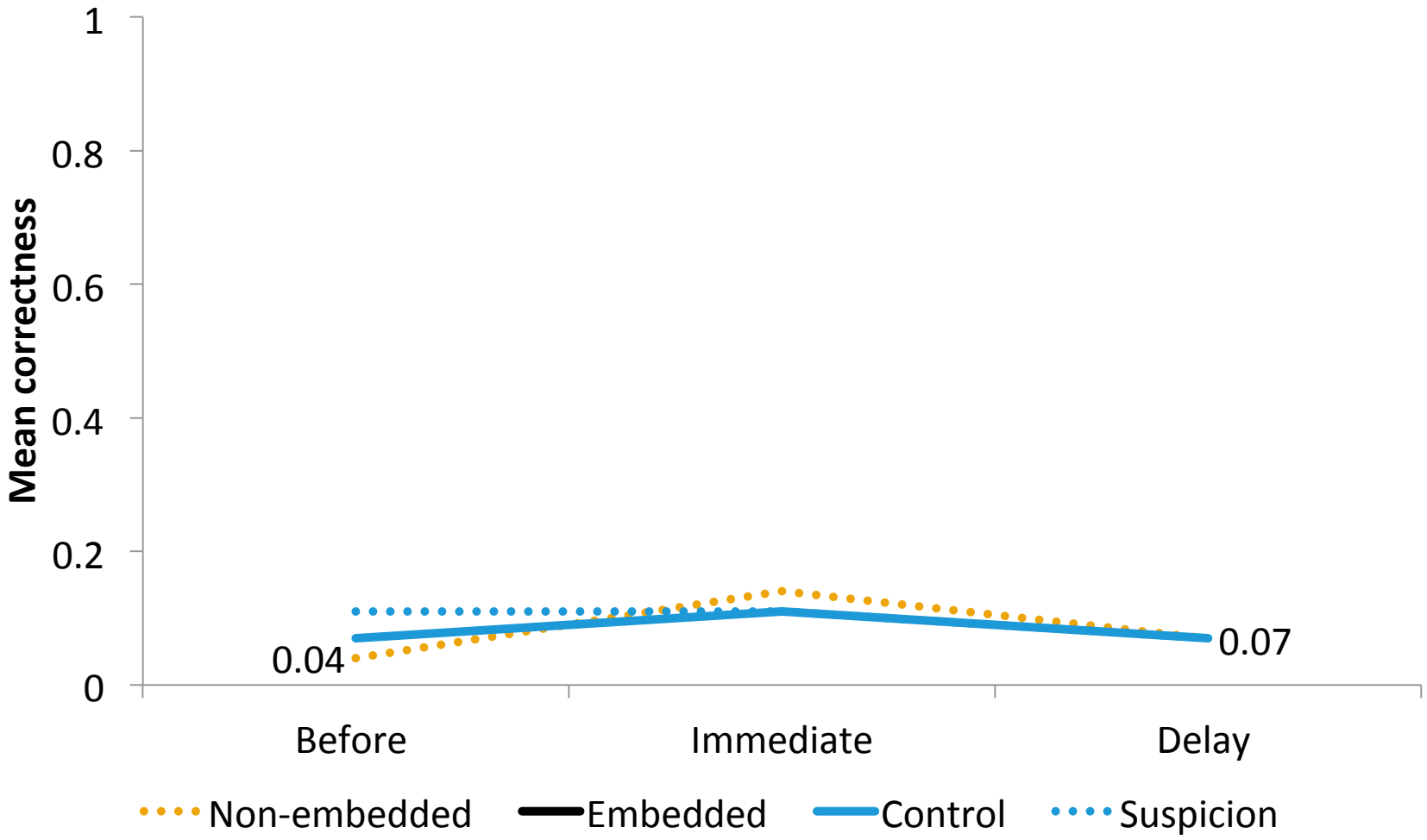
Data analysis

- We treated clicking on link to be falling for phishing
- 89% of the users who clicked went ahead and gave personal information

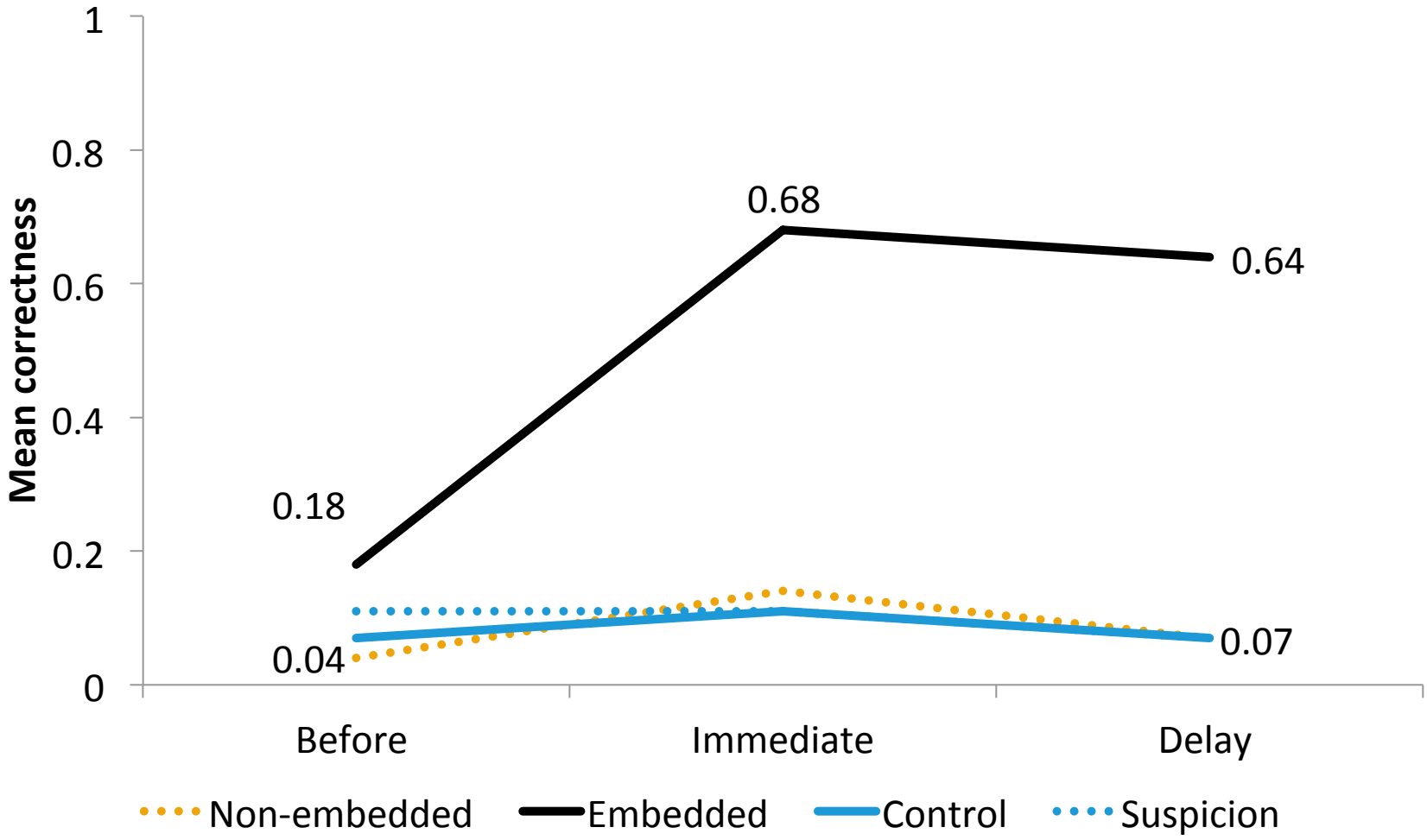
Results - Phishing account emails



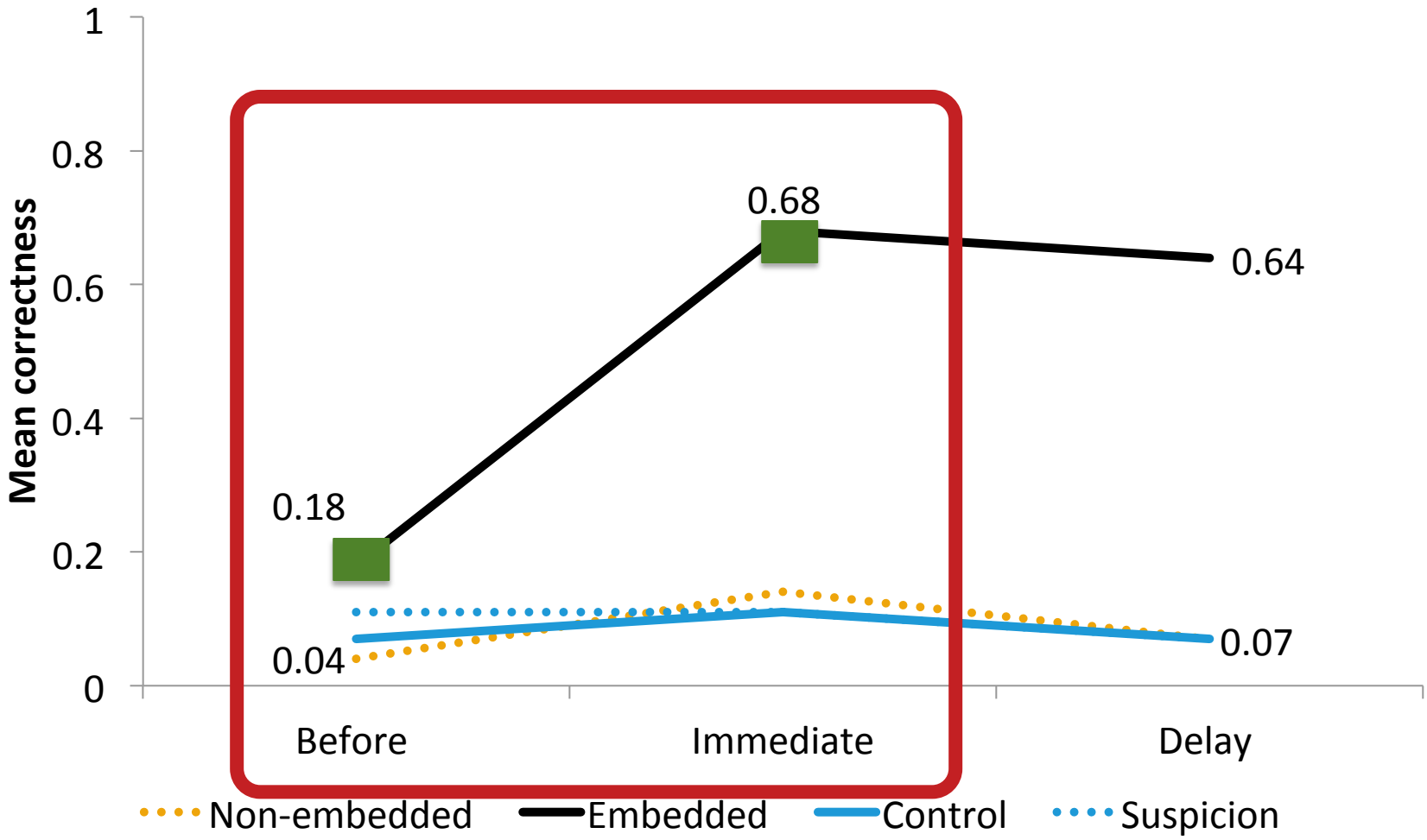
Results - Phishing account emails



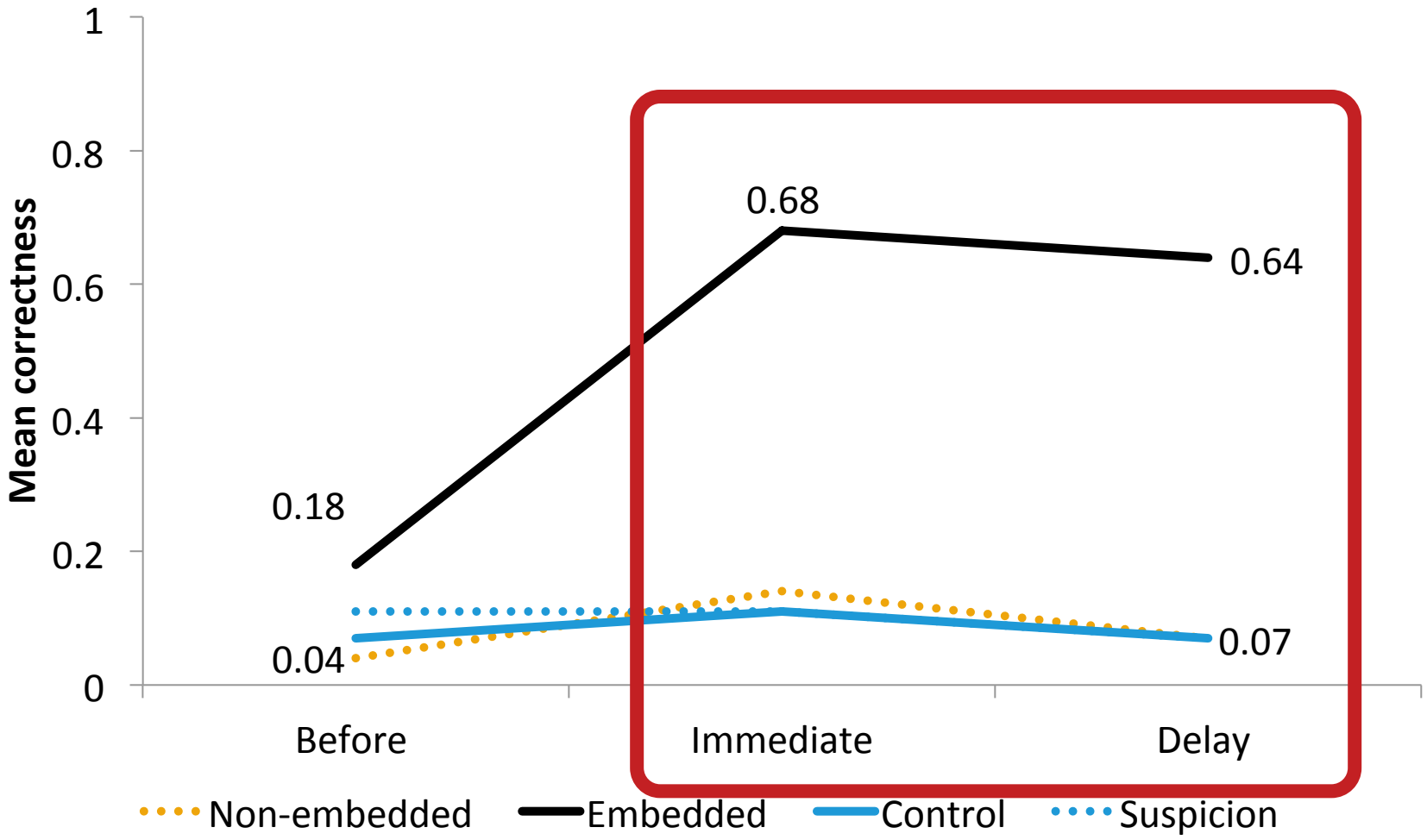
Results - Phishing account emails



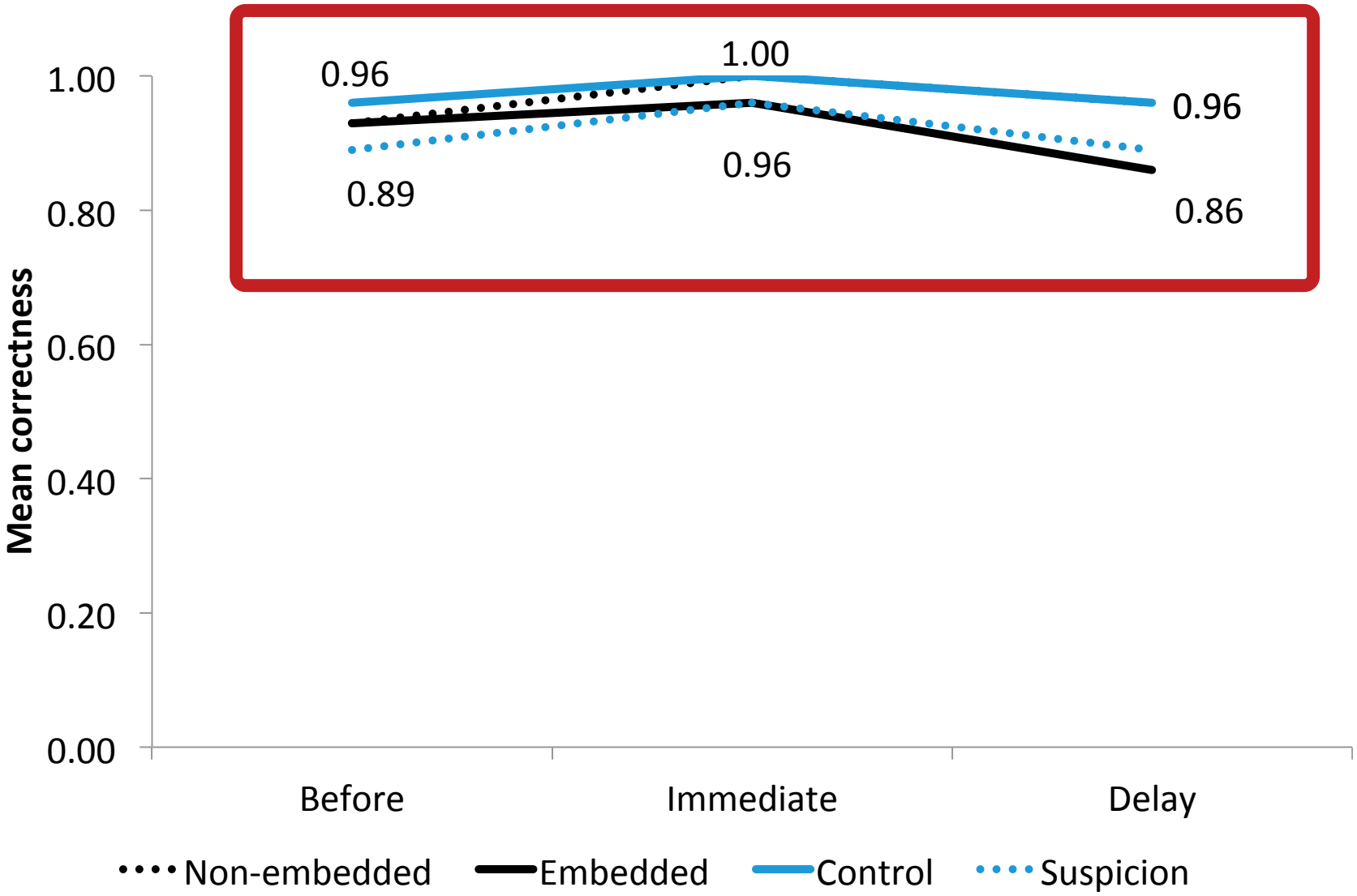
Results - Phishing account emails



Results - Phishing account emails



Results – Legitimate link emails



Participant quote

- “I was more motivated to read the training materials since it was presented after me falling for the attack.”

Real world study: CMU

- Evaluate effectiveness of PhishGuru training in the real world
- Investigate retention after 1 week, 2 weeks, and 4 weeks
- Compare effectiveness of 2 training messages with effectiveness of 1 training message

P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of Phish: A Real-World Evaluation of Anti-Phishing Training. *SOUPS 2009.*

Study design

- Sent email to all CMU students, faculty and staff to recruit participants to opt-in to study
- 515 participants in three conditions
  - Control
  - One training message
  - Two training messages
- Emails sent over 28 day period
  - 7 simulated spear-phishing messages
  - 3 legitimate messages from ISO (cyber security scavenger hunt)
- Exit survey

Implementation

- Unique hash in the URL for each participant
- Demographic and department/status data linked to each hash
- Form does not POST login details
- Campus help desks and all spoofed organizations were notified before messages were sent

Study schedule

Day of the study	Control	One training message	Two training messages
Day 0	Test and real	Train and real	Train and real
Day 2	Test		
Day 7	Test and real		
Day 14	Test	Test	Train
Day 16	Test		
Day 21	Test		
Day 28	Test and real		
Day 35	Post-study survey		

Simulated spear phishing message

From: Help Desk <alert-password@cmu.edu>
Subject: **Your Andrew password alert**
Date: November 17, 2008 11:08:19 AM EST
To: Ponnurangam Kumaraguru (PK)

Plain text email without graphics

Dear Student/Faculty/Staff,

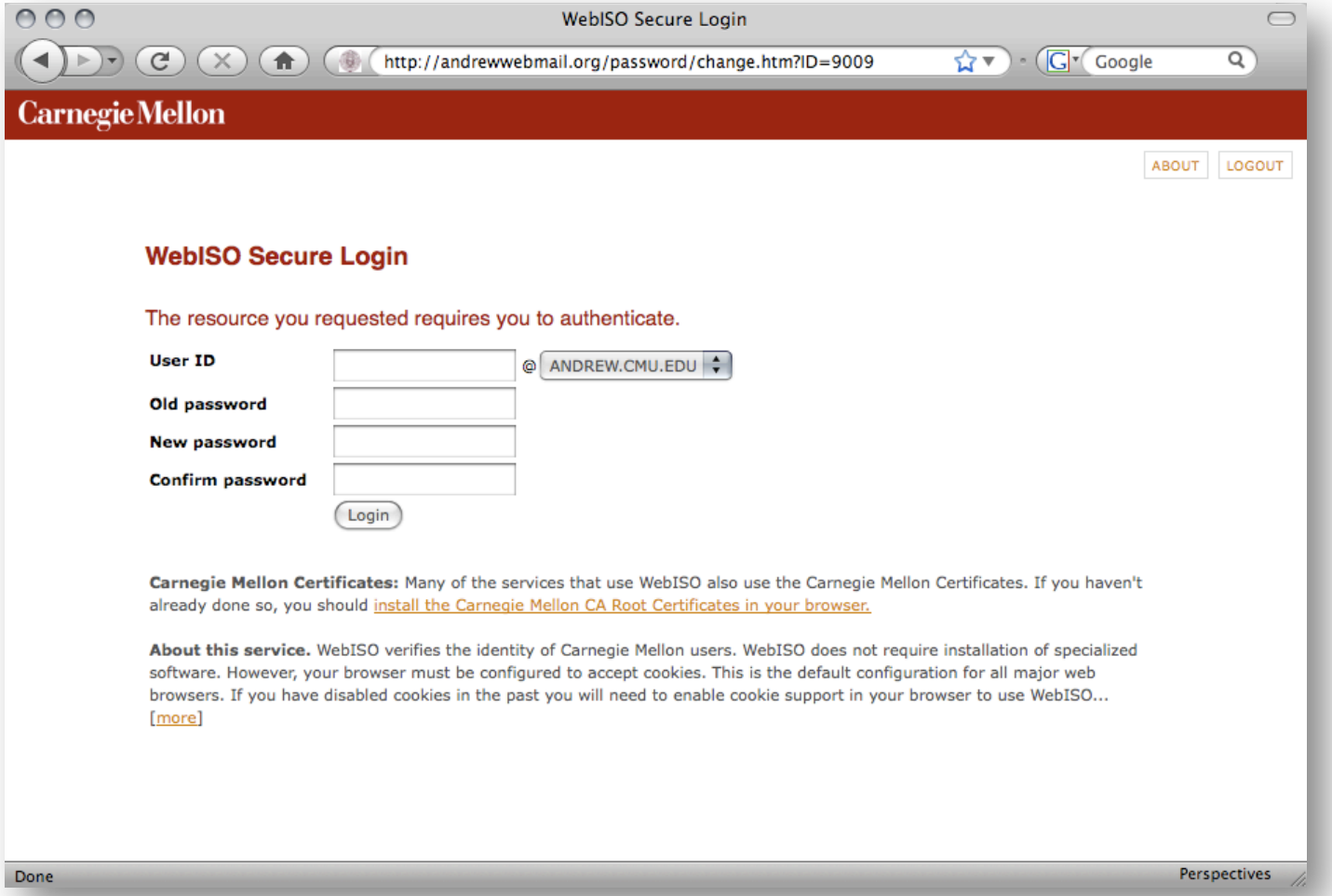
Our records indicate that you have not changed your Andrew password in the last 90 days, if you do not change your password in the next 5 days, your access to the Andrew email system will be terminated. Click the link below to update your password.

http://andrewwebmail.org/password/change.htm?ID=9009

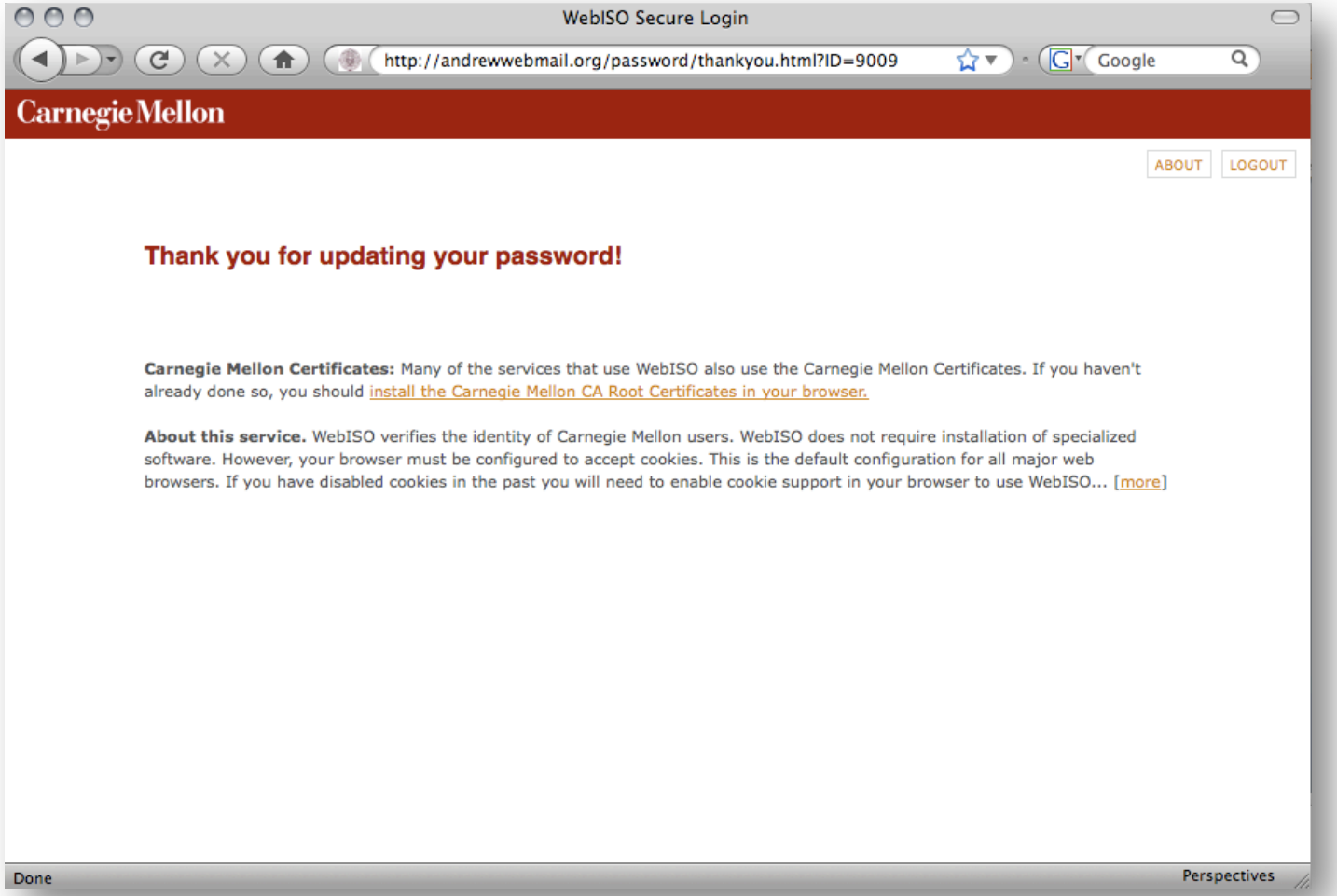
URL is not hidden

Sincerely,
Andrew Help Desk

Simulated phishing website



Simulated phishing website



PhishGuru intervention

Simulated phishing emails

From	Subject line
Info Sec	Bandwidth Quota Offer
Networking Services	Register for Carnegie Mellon's annual networking event
Webmaster	Change Andrew password
The Hub - Enrollment Services	Congratulation - Plaid Ca$h
Sophie Jones	Please register for the conference
Community Service	Volunteer at Community Service Links
Help Desk	Your Andrew password alert

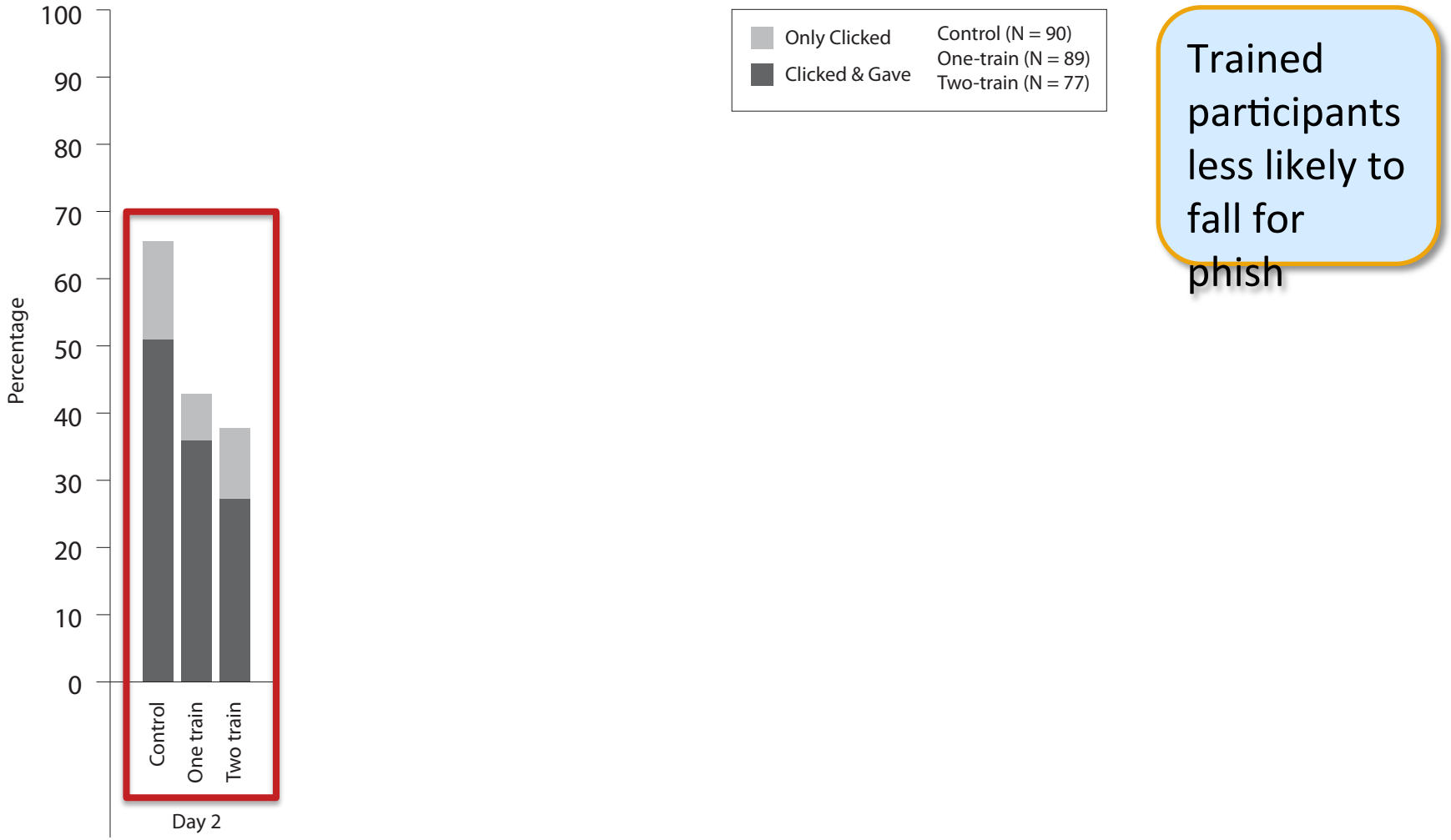
Results

- People trained with PhishGuru were less likely to click on phishing links than those not trained
- People retained their training for 28 days
- Two training messages are better than one
- PhishGuru training does not make people less likely to click on legitimate links
- Age was most significant factor in determining vulnerability

Effect of PhishGuru

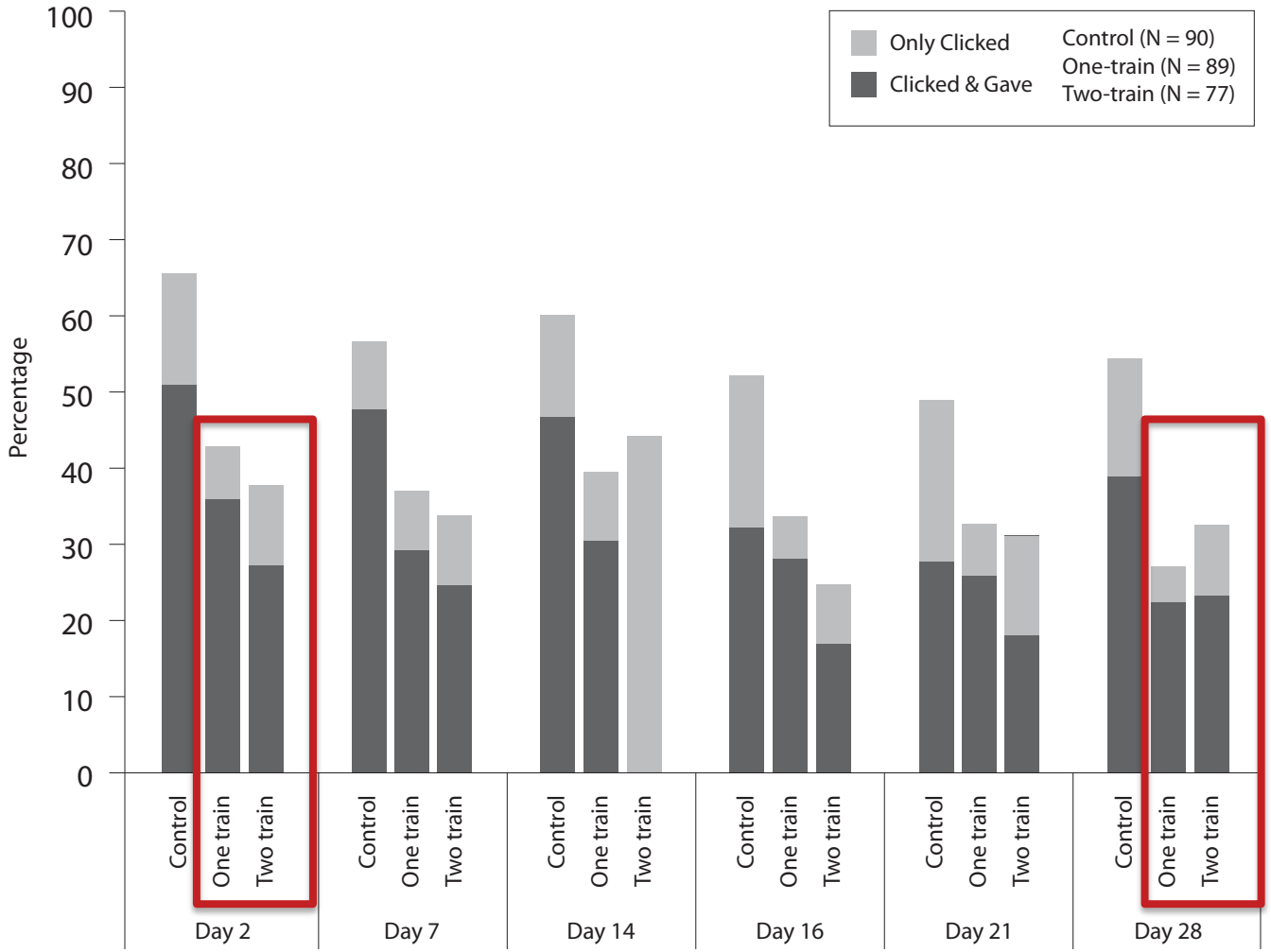
Condition	N	% who clicked on Day 0	% who clicked on Day 28
Control	172	52.3	44.2
Trained	343	48.4	24.5

Results conditioned on participants who clicked on day 0



Trained participants less likely to fall for phish

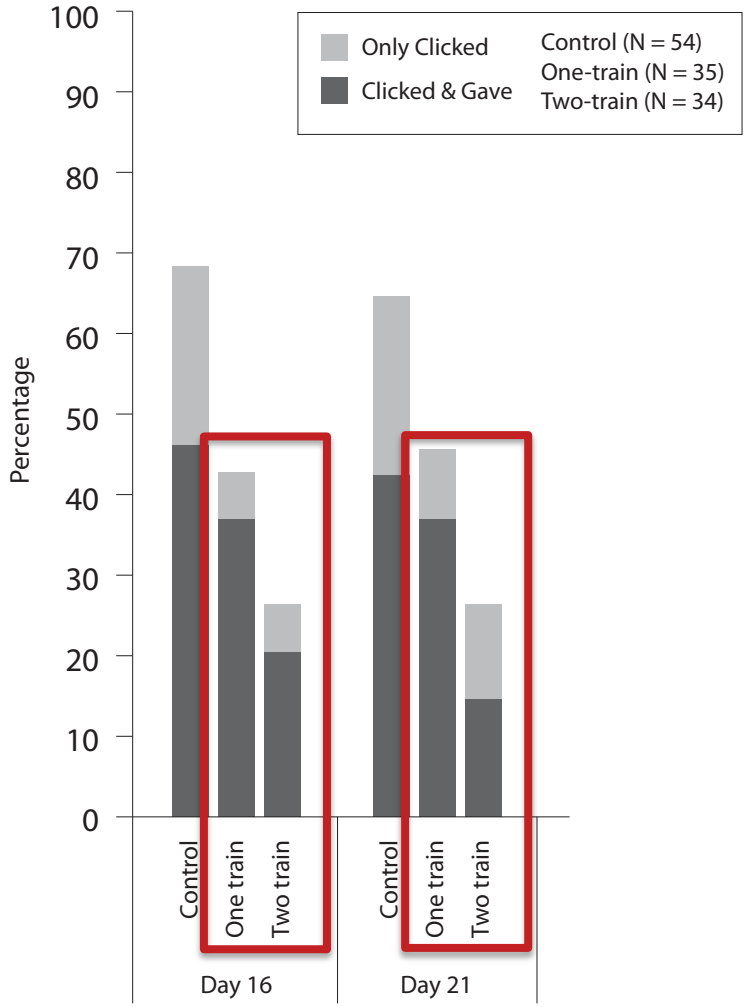
Results conditioned on participants who clicked on day 0



Trained participants less likely to fall for phish

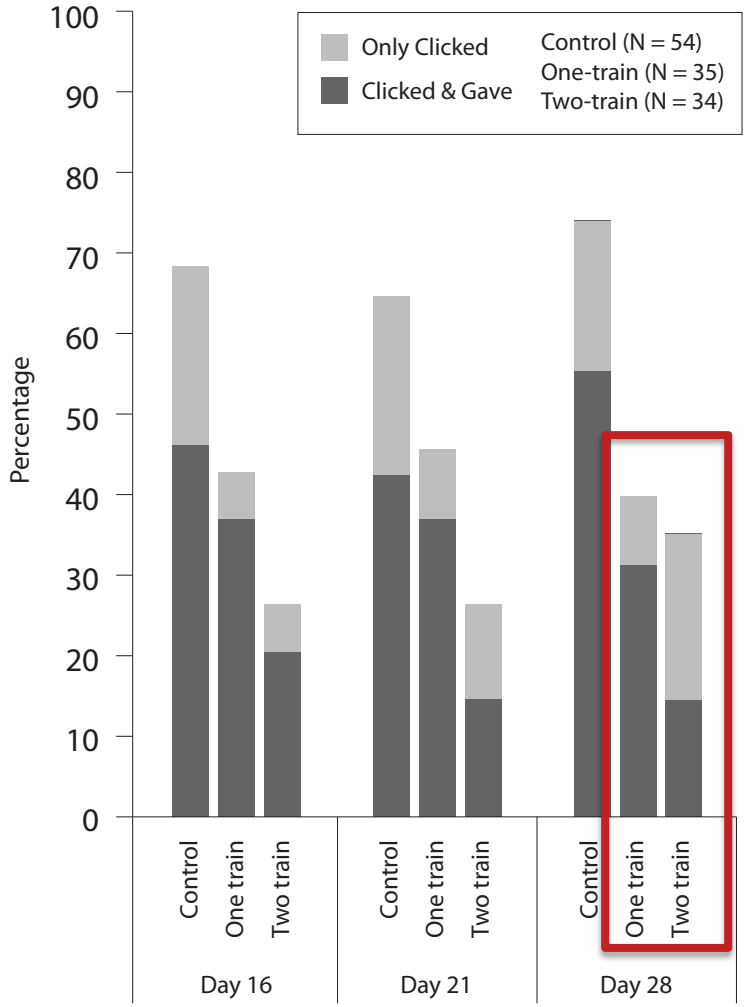
Trained participants remember what they learned 28 days later

Results conditioned on participants who clicked on day 0 and day 14



Two-train participants less likely than one-train participants to click on days 16 and 21

Results conditioned on participants who clicked on day 0 and day 14



Two-train participants less likely than one-train participants to click on days 16 and 21

Two-train participants less likely than one-train participants to provide information on day 28

Legitimate emails

Condition	N	Day 0	Day 7	Day 28
		Clicked %	Clicked %	Clicked %
Control	90	50.0	41.1	38.9
One-train	89	39.3	42.7	32.3
Two-train	77	48.1	44.2	35.1

No difference between the three conditions on day 0, 7, and 28

Legitimate emails

Condition	N	Day 0	Day 7	Day 28
		Clicked %	Clicked %	Clicked %
Control	90	50.0	41.1	38.9
One-train	89	39.3	42.7	32.3
Two-train	77	48.1	44.2	35.1

No difference between the three conditions on day 0, 7, and 28

No difference within the three conditions for the three emails

Students are most vulnerable

- Students significantly more likely to fall for phish than staff before training
- No significant differences based on student year, department, or gender
- 18-25 age group were consistently more vulnerable to phishing attacks on all days of the study than older participants

Percentage who clicked by age group

Age group	Day 0
18-25	62%
26-35	48%
36-45	33%
45 and older	43%

Most participants liked training, wanted more

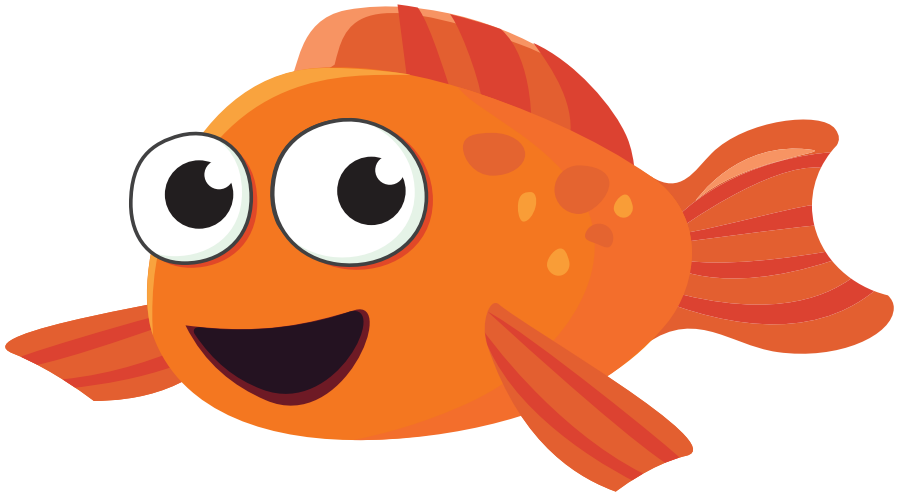
- 280 completed post study survey
- 80% recommended that CMU continue PhishGuru training
  - “I really liked the idea of sending CMU students fake phishing emails and then saying to them, essentially, HEY! You could've just gotten scammed! You should be more careful - here's how....”
  - “I think the idea of using something fun, like a cartoon, to teach people about a serious subject is awesome!”

APWG landing page

- Train people when they fall for actual phishing emails
- Redirect people to “landing page”
- CMU collecting and analyzing log files
- P. Kumaraguru, L. Cranor, and L. Mather. Anti-Phishing Landing Page: Turning a 404 into a Teachable Moment for End Users. CEAS 2009. http://www.ceas.cc/papers-2009/ceas2009-paper-37.pdf

- http://education.apwg.org/

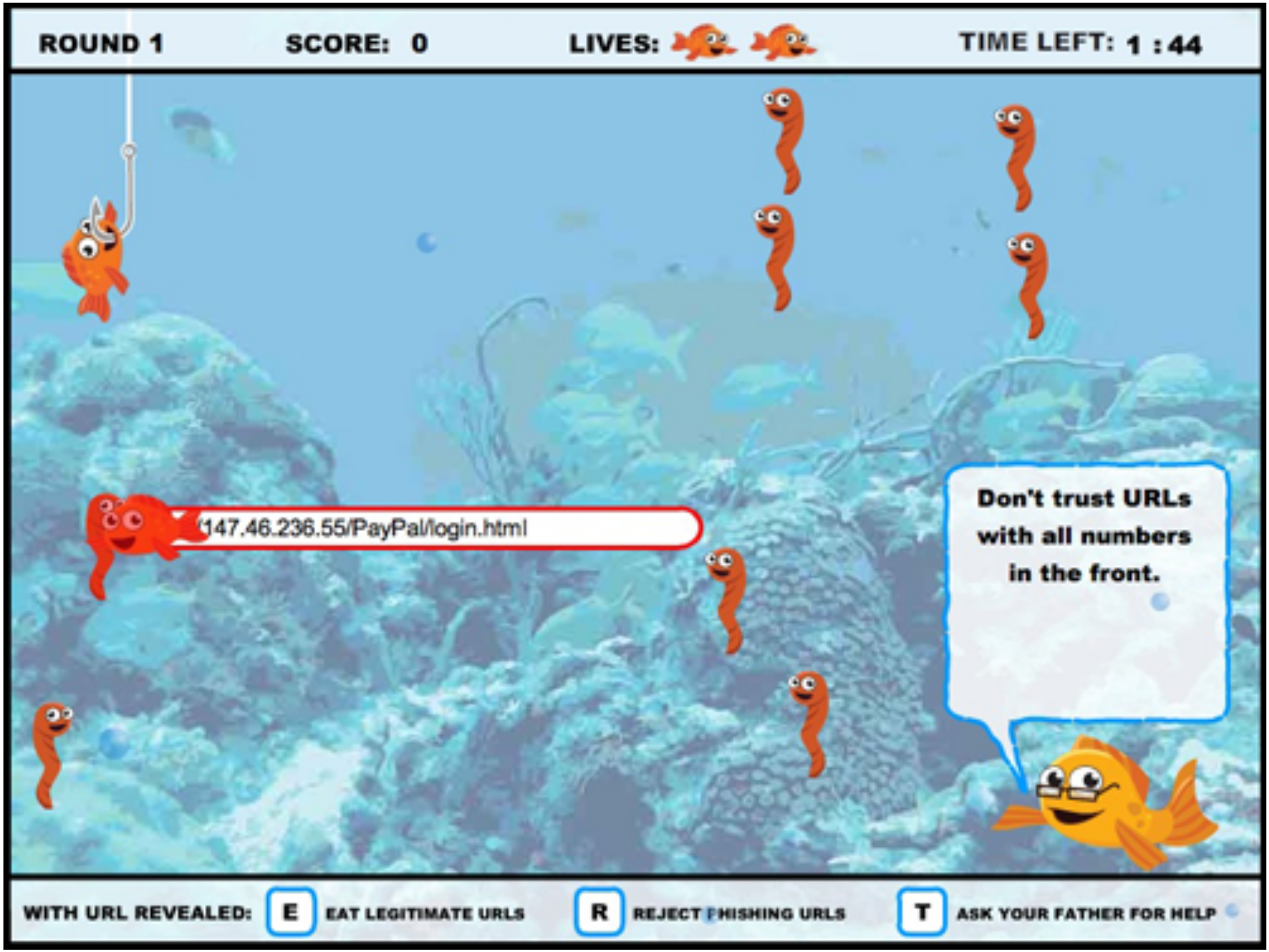
Anti-phishing Phil



Anti-Phishing Phil

- Online game
- http://wombatsecurity.com/antiphishingphil
- Teaches people how to protect themselves from phishing attacks
  - identify phishing URLs
  - use web browser cues
  - find legitimate sites with search engines

S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 2007 Symposium On Usable Privacy and Security,* Pittsburgh, PA, July 18-20, 2007.


ROUND 1
SCORE: 0
LIVES:
TIME LEFT: 1 : 44
147.46.236.55/PayPal/login.html
Don't trust URLs with all numbers in the front.
WITH URL REVEALED:
E
EAT LEGITIMATE URLS
R
REJECT PHISHING URLS
T
ASK YOUR FATHER FOR HELP

ROUND 1 ... ME LEFT:

ROUND OVER

Congratulations! You May Proceed to the Next Round

(✓) correct choice (✗) incorrect choice

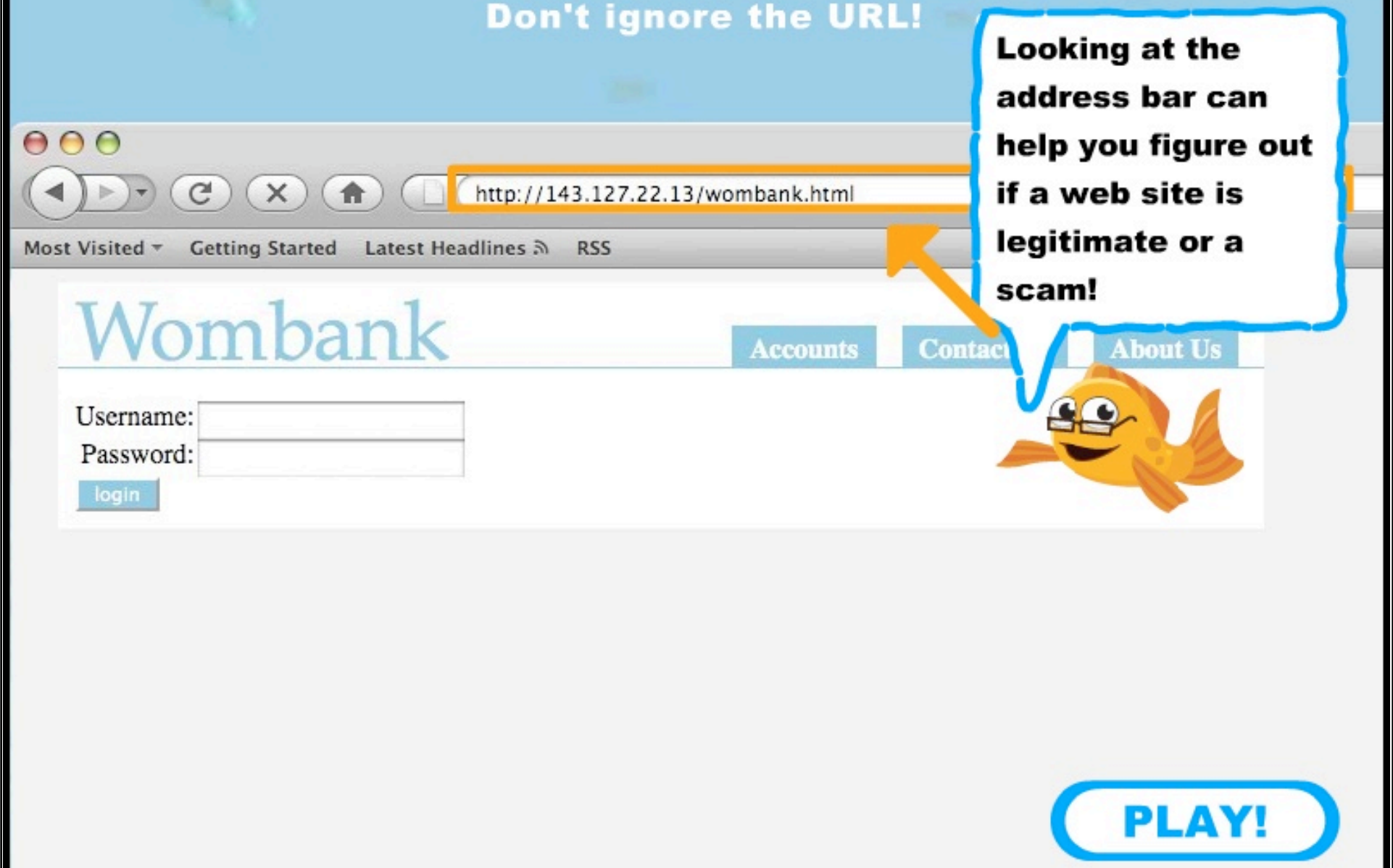
✓	http://165.246.121.80/wamu/	SCAM ALERT! URLs with all numbers in the front are usually scam.
✓	http://www.msn-verify.com/	SCAM ALERT! keywords such as verify, update in the domain usually means it is scam.
✓	http://www.chase.com	Chase.com is part of the J.P. Chase Corporation.
✓	https://www3.nationalgeographic.com/	Don't be fooled by the www3, this site belongs to nationalgeographic.com
✓	http://www.onlineregionsbank.com/	SCAM ALERT! Regions bank website is regions.com, not onlineregionsbank.com
✓	http://www.citizensbank.com	citizensbank.com belongs to Citizens Bank.
✗	http://147.91.75.1/ebay/	SCAM ALERT! URLs with all numbers in the front are usually scam.
✗	http://www.amazon.com	amazon.com is the shopping site Amazon.

WITH URL REVEALED: E EAT LEGITIMATE ... G URLS T ASK YOUR FATHER FOR HELP

NEXT ROUND

How To Avoid Online Scams

Don't ignore the URL!



User Study

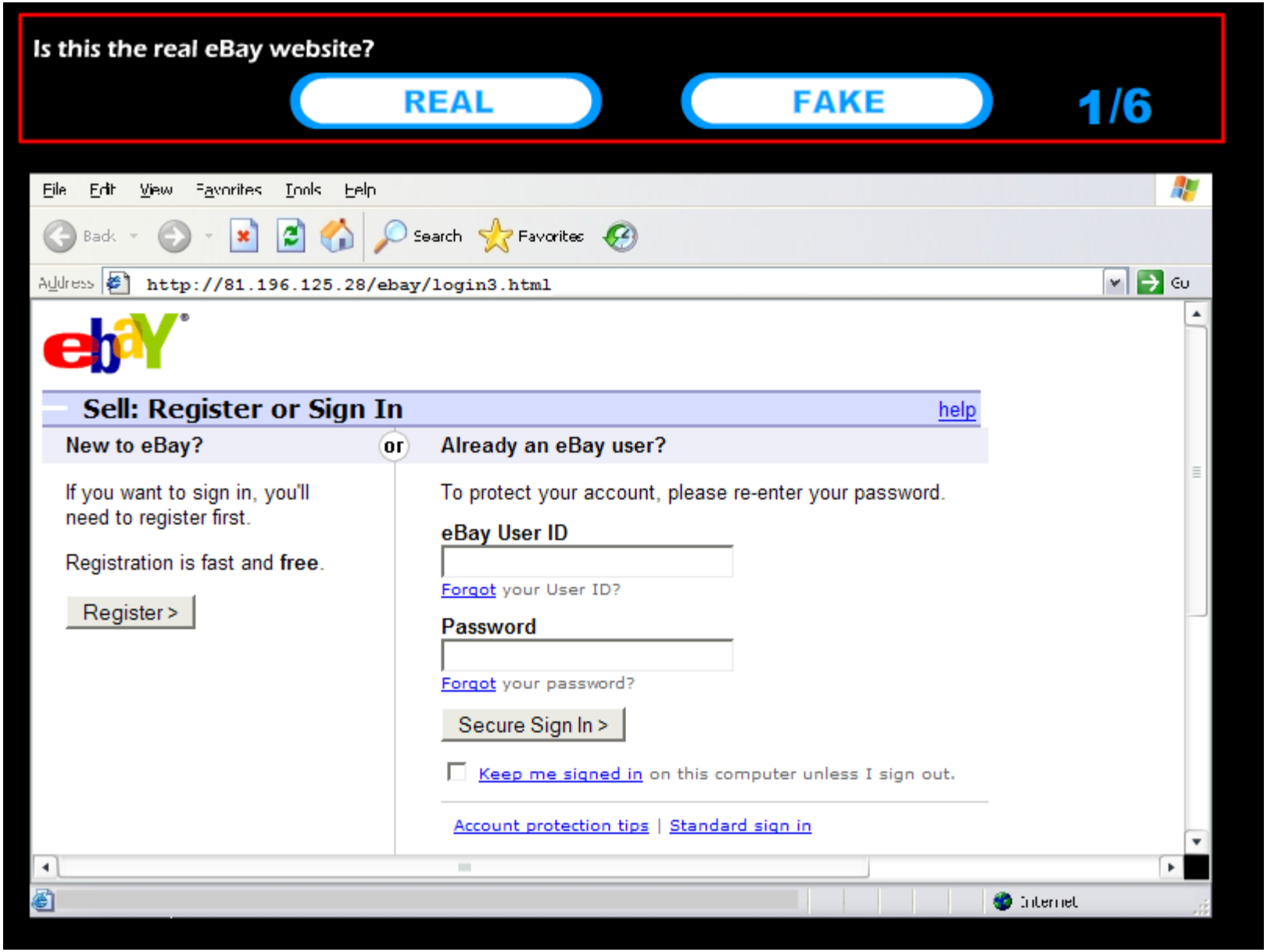
- Test participants' ability to identify phishing web sites before and after training
  - 10 URLs before training, 10 after, randomized
  - Up to 15 minutes of training
- Three conditions:
  - Web-based phishing education
  - Tutorial
  - Game
- 14 participants in each condition
  - Screened out security experts
  - Younger, college students

Results

- No significant difference in false negatives among the three groups
- Game group performed best in false positives
- All training we tested made people more suspicious, but only the game helped people distinguish phish from legitimate web sites

Field Study

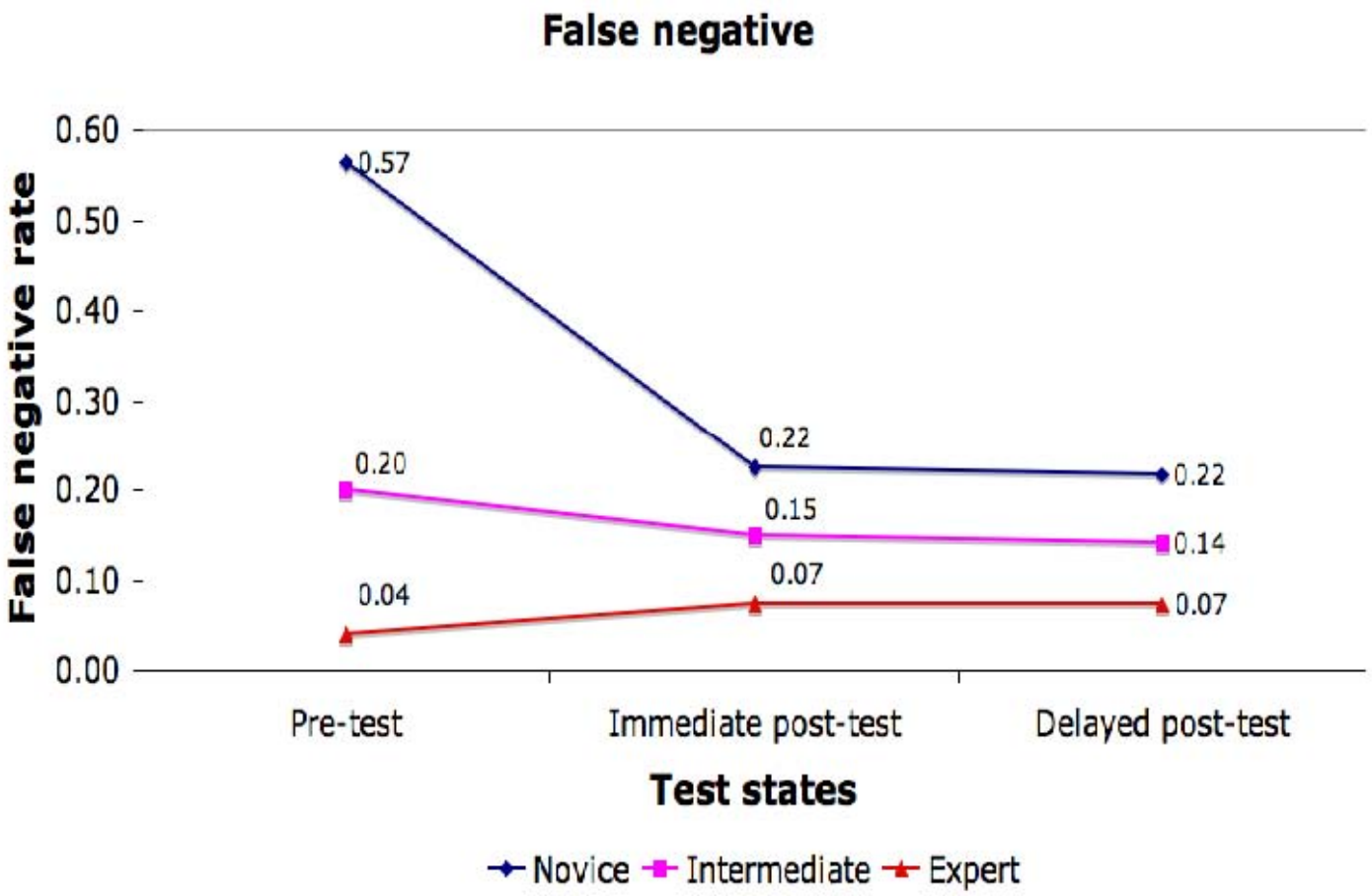

Help Us With Our Research!
Enter to win a $100 Amazon gift certificate!!!
Take a short 6-question phishing quiz before you play the game, another 6-question quiz after you play the game, and another 6- question quiz one week later for a chance to win a $100 Amazon gift certificate. The quizzes and game should take about 12 minutes. If you get at least 80% of the quiz questions right you will get an extra raffle ticket.
We will record your quiz scores and answers to the survey questions and use them in our research. However your scores and responses will not be identified with your name.
You must be 13 or older to participate.
CONTINUE
SKIP SURVEY


Is this the real eBay website?
REAL
FAKE
1/6
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://81.196.125.28/ebay/login3.html
Go
ebay
Sell: Register or Sign In
help
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
To protect your account, please re-enter your password.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Secure Sign In >
Keep me signed in on this computer unless I sign out.
Account protection tips | Standard sign in
Internet

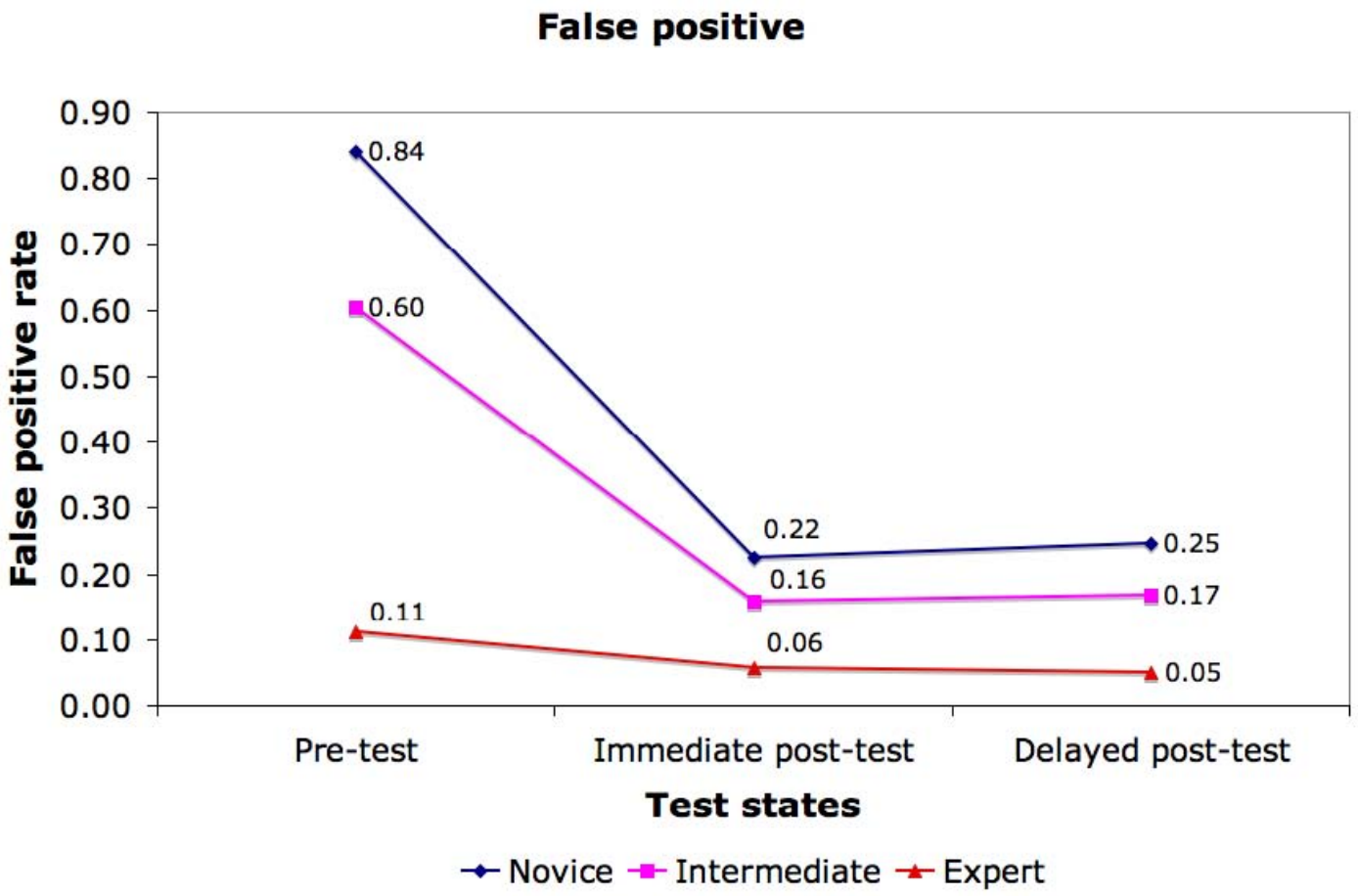
Study Set-up

- Test participants' ability to identify phishing web sites after training and the ability to retain the knowledge
  - 6 URL quiz
    - before training, after training, one week later
- Conditions:
  - Control
  - Game
- Completed training
  - 2,021 in training group
    - 674 returned one week later
  - 2,496 in control group

False negative results



False positive results



Comments

- “I liked the game! It was fun to play and had a useful message.”
- “Excellent game. Getting people to actually learn is the tough part.”
- “Is it available to training facilities for use with Corporate compliance and Internet training classes?”
- “I plan to direct my mother to this site.”

Coolest Security Tool Ever! - Online game to teach cyber-security

By: Alexandru Dumitru, Security News Editor

Enlarge picture

Now this is certainly something really nice! Researchers are advising users kindergarden-style! These people are going out of their way to help people stay secure. Of course, the best way of protecting yourself against the threats on the web is to know what they are and how to act against them. That's why the brainy dudes at Carnegie Mellon University have designed a game to help people out!

Now, I knew that some warnings and pieces of news were for the tech-savvy users that knew too much about security already, but they're dumbing down security measures so much that even a 10-year-old could stay safe on the web. If this doesn't make a difference, then I don't know what will!

The game is called Anti-Phishing Phil, and you can play it by clicking on this link. Not only is it entertaining – I really like that fish – but it's also going to teach you a lot. So, this is a great initiative – these people are making it stupid-proof – web users should understand phishing threats and know how to watch out against them a lot better after playing the game. And you can play it just for fun, if you're a security geek. Or you can play it just to test your knowledge – in any case, I like this initiative a lot.

I've seen a similar thing on Agnitum's website – it's a quiz that will tell you if you're a security wizard or not. That was pretty cool, but this fish beats the crap out of any other web threat awareness tool ever!

Be my guest and click on the link above to Anti-Phishing Phil. You're bound to like it! And I wonder what's next, are researchers going to come up with a game with "Sexy Lisa" warning against "porn-related spam"?

Homepage – Banca Popolare di Sondrio

http://www.popso.it/home

Google

English | Contatti | Accessibilità | A A A cerca

Banca Popolare di Sondrio

HOME | CHI SIAMO | INFORMATIVA SOCIETARIA | CULTURA E TERRITORIO | PRODOTTI E SERVIZI | MONDO ESTERO

PHIL, IL PESCE "ANTI PHISHING"

La sicurezza on line non è un gioco... con il pesce PHIL può scoprire come proteggersi dal *phishing*!

Accedi a SCRIGNO*Internet Banking*

SCRIGNO*Internet Banking*: i nostri servizi bancari sempre a portata di mano:
Scopri il servizio

BANCA&WEB

- Banca Popolare di Sondrio (SUISSE)
- Tempo libero e webcam
- Le nostre iniziative culturali
- Navigosereno.it - sicurezza on line

COMUNICATISTAMPA

- Assemblea dei Soci - Esercizio 2008
- Banca Popolare di Sondrio si rinnova nel web

MONDOESTERO

- Sistemi di pagamento
- Internazionalizzazione
- Imprese e mercati esteri

IN EVIDENZA

SCRIGNOmobile
La nostra soluzione per avere la banca 'in tasca', grazie alla navigazione dal proprio telefonino o tramite SMS.

TEMPO LIBERO

Trekking, mountain bike e rifugi in Valtellina e zone limitrofe

IL NUOVO SITO

Una guida per orientarsi

SERVIZI ON LINE

Un approfondimento della nostra offerta on line

Ultimo aggiornamento: 02.04.2009

[INIZIATIVA DELLA BANCA POPOLARE DI SONDRIO]

Proteggersi dai furti in "rete" con Phil è un gioco da ragazzi

Per combattere spam e frodi in internet oggi c'è un efficace anti-phishing

DELEBIO Proteggersi dai furti di dati sensibili attraverso accorgimenti informatici e posta certificata, ma anche attraverso "Phil, il pesce anti-phishing". Presso la filiale delebiese della Banca Popolare di Sondrio è stato presentato ieri mattina un nuovo programma-gioco educativo rivolto a utenti e dipendenti per imparare a riconoscere e difendersi dai ladri di dati personali. «Abbiamo puntato decisamente all'accessibilità ai servizi da parte dei nostri clienti attraverso i più diversi canali - ha spiegato il vicedirettore generale di Bps, Milo Gusmeroli - e la sicurezza è caratteristica indispensabile per la diffusione di sistemi come quello delle operazioni bancarie on line. Fino ad oggi siamo riusciti a fronteggiare i rischi che gli utenti corrono in internet ma la guardia rimane alta e per questo dopo Navigo sereno" abbiamo scelto di lanciare Phil come metodo di prevenzione e informazione per utenti e dipendenti».
L'ispettore capo della polizia delle comunicazioni di Sondrio, Valter Fumasoni insieme a Ivan Lorez hanno spiegato le origini del phishing «che rappresenta il furto di dati sensibili attraverso errori di programmazione che rendono vulnerabile il sistema».
Tra le indicazioni date per difendersi da e-mail e messaggi falsi, c'è quella di non fornire mai dati richiesti attraverso la posta elettronica, e di dotarsi di una mail certificata che sia cioè identificabile con certezza di provenienza. Il rischio, in caso di phishing, è che ottenendo i dati dell'utente possano essere effettuate operazioni quali prelievi e trasferimenti di denaro dal proprio conto verso l'estero. Il responsabile dei sistemi innovativi di Bps, Marco Tempra, ha sottolineato che «per fronteggiare le vulnerabilità tecniche e umane il gioco educativo Phil, il pesce anti-phishing avrà un ruolo importante nei programmi di formazione atti a prevenire le frodi e sensibilizzare i clienti. Alcuni anni fa abbiamo lanciato il sito www.navigosereno.it, che consente di trovare consigli, informazioni e software per la sicurezza del pc dei clienti. Phil, quale componente della nostra linea strategica sui temi della sicurezza on line, si concentrerà sulla formazione, con una versione limitata per il pubblico sul sito www.popso.it/sicurezza, e la versione completa riservata ai clienti nel servizio on line Scrigno internet banking. Il gioco ha dimostrato di essere significativamente più efficace nel formare le persone a riconoscere gli attacchi di phishing rispetto alle più tradizionali soluzioni presenti sul mercato.

Annalisa Acquipastapace

RELAX NEL LAGHETTO
Dopo la presentazione nella filiale delebiese della Banca Popolare, tutti al laghetto di Piantedo FOTO SANDONINI

Why is Phil so popular?

- Addresses a problem people are concerned about
- Fun to play
- People like to win things (or even just get points)
- Get trained fast (about 10 minutes)
- Teaches actionable steps
- Interactive, reinforces learning

Security user education is possible

- Conventional wisdom: end-user security training does not work
- Our work shows otherwise
  - You can teach Johnny not to fall for phish
- We should still aim to reduce or eliminate computer security threats through technology and enforcement
- But these efforts should be complemented with user education