Results from "Help Us Protect the Carnegie Mellon Community from Identity Theft" study

A Real-Word Evaluation of Anti-Phishing Training

Mary Ann Blair
Lorrie Faith Cranor
Ponnurangam Kumaraguru (PK)

Joint work with Justin Cranshaw, Alessandro Acquisti, Jason Hong, and Theodore Pham

Carnegie Mellon

CyLab Usable Privacy and Security Laboratory
http://cups.cs.cmu.edu/

Outline

- Motivation for collaboration
- Phishing 101
- PhishGuru
- CMU-PhishGuru study design and results
- How to protect yourself
- Lessons learned

Motivation for collaboration

Security Alert - Fraud Emails - CARNEGIE MELLON UNIVERSITY INTERNET USER
(Posted September 29, 2008)

Fraud emails have recently been sent to Carnegie Mellon email accounts claiming to be from *Carnegie Mellon University <cmu@webmaster.com>*. The fraud messages ask people to reply with their *Full Name, User Id, and Password*. **PLEASE ENABLE SPAM FILTERING AND DO NOT REPLY!**
For **What You Need To Do**, see Security Alert - Fraud Emails - CARNEGIE MELLON UNIVERSITY INTERNET USE.

www.cmu.edu/iso

Motivation for collaboration

Security Alert - Fraud Emails - andrew.cmu.edu Feature Release: Upgraded Search
(Posted August 27, 2008)

Fraud emails have recently been sent to Carnegie Mellon email accounts claiming to be from *memberservice@andrew.cmu.edu*. The fraud messages ask people to reply with their *User ID and Password*. **PLEASE ENABLE SPAM FILTERING AND DO NOT REPLY!**
For **What You Need To Do**, see Security Alert - Fraud Emails - andrew.cmu.edu Feature Release: Upgraded Search.

www.cmu.edu/iso

Motivation for collaboration

- Reduce risk
  - identity theft
  - credential stealing
  - data leakage
- Improve operational effectiveness
- Support research
- Help individuals avoid being scammed

Phishing 101

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 re-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:

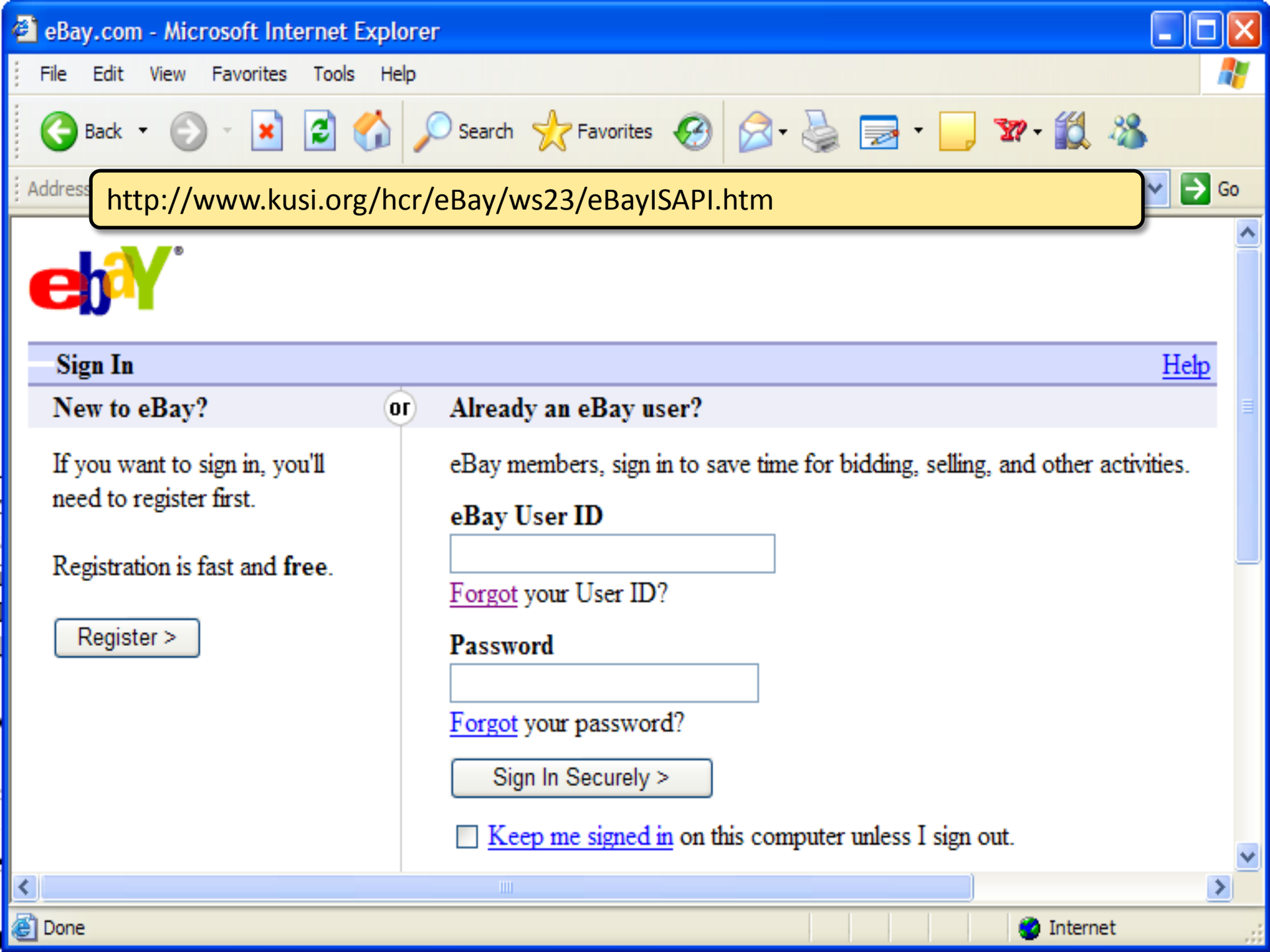
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&sidteid=0

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

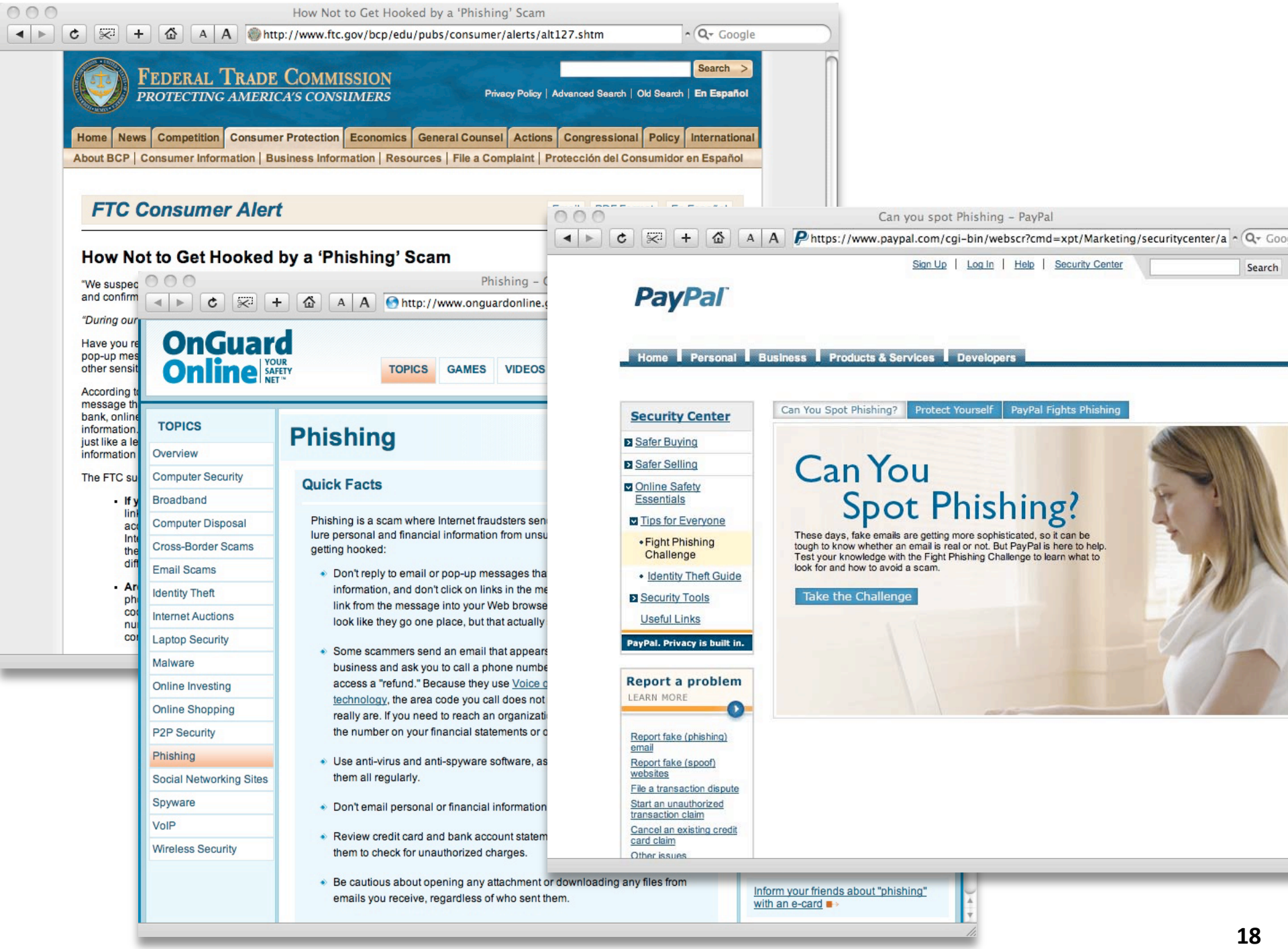
- For most users, security is a secondary task
- It is difficult to teach people to make the right online trust decision without increasing their false positive errors

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.** In Proceedings of the 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]

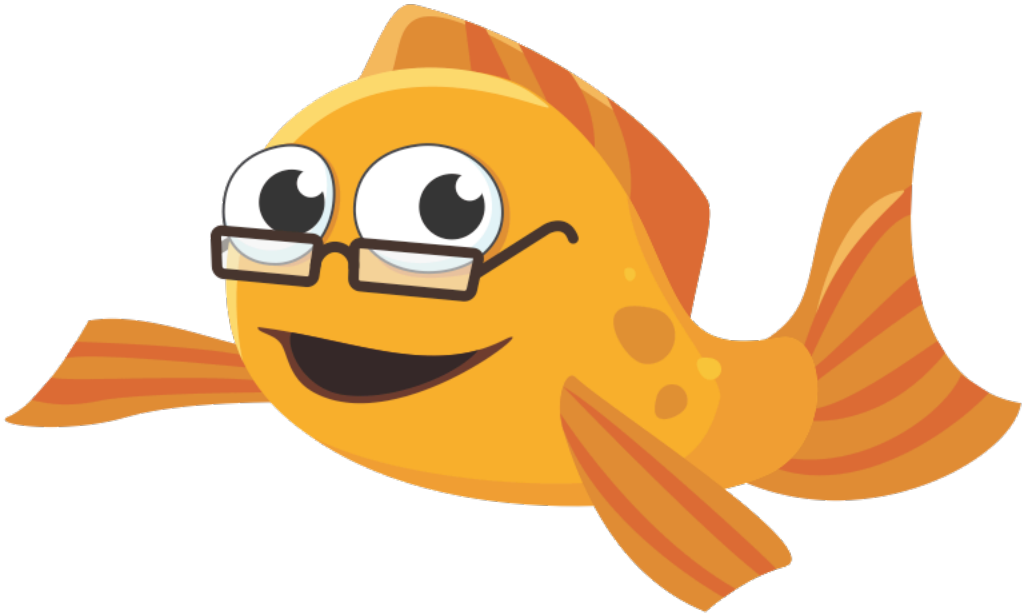

How Not to Get Hooked by a 'Phishing' Scam
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm
Google
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Search
Privacy Policy | Advanced Search | Old Search | En Español
Home | News | Competition | Consumer Protection | Economics | General 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
Phishing
http://www.onguardonline.
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
Phishing
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
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

Web site training study

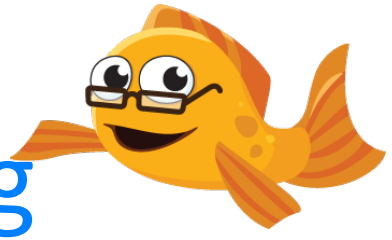
- Laboratory study of 28 non-expert computer users
- Control group: evaluate 10 sites, 15 minute break to read email or play solitaire, evaluate 10 more sites
- Experimental group: evaluate 10 sites, 15 minutes to read web-based training materials, evaluate 10 more sites
- Experimental group performed significantly better identifying phish after training
  - But they had 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. CyLab Technical Report CMU-CyLab-07003, 2007.

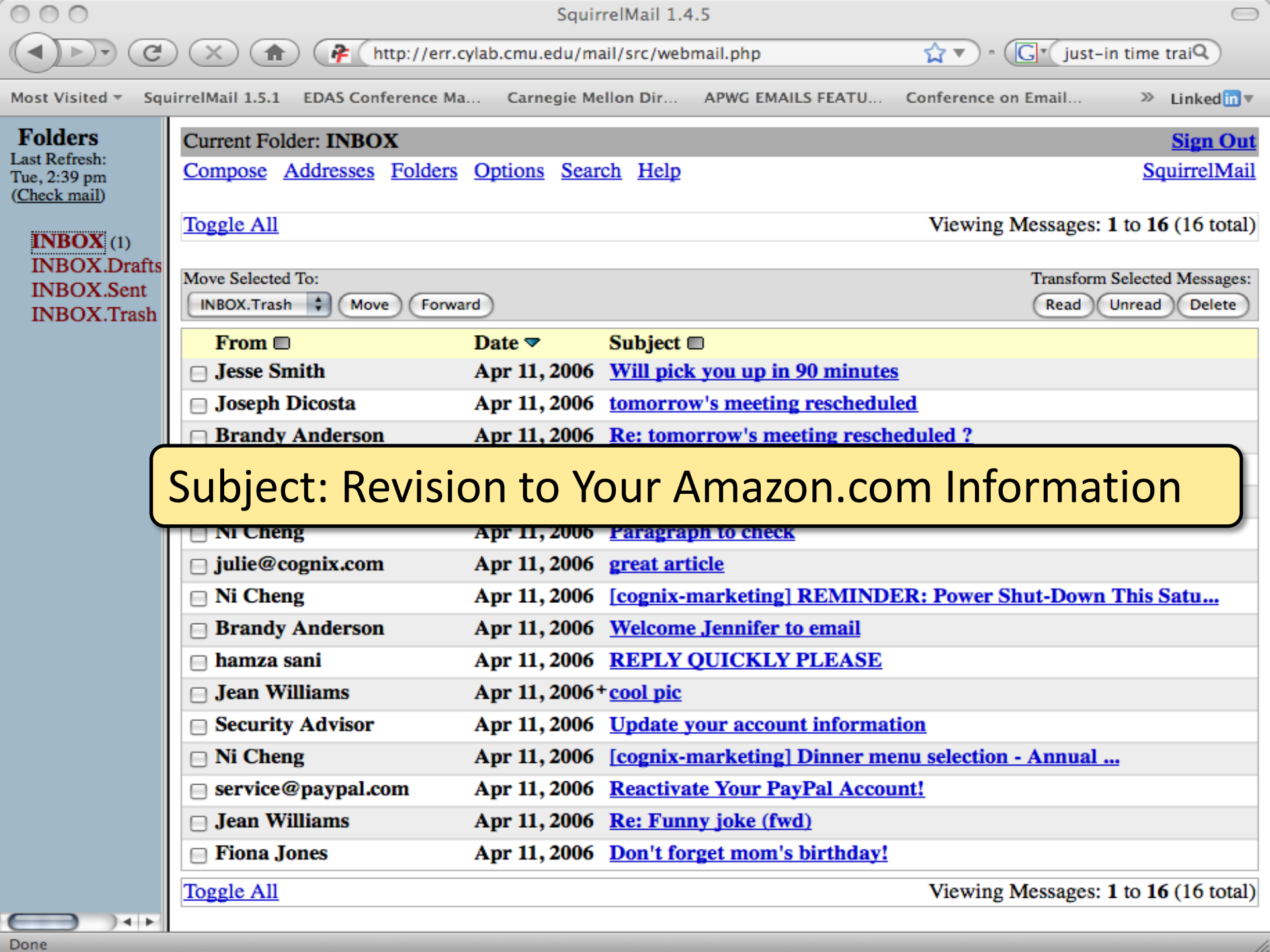
PhishGuru



PhishGuru Embedded Training



- Can we "train" people during their normal use of email to avoid phishing attacks?
  - Periodically, people receive a training email
  - Training email looks like a phishing attack
  - If a person falls for it, intervention warns and highlights what cues to look for in succinct and engaging format
- Motivating users – "teachable moment"
- Applies learning science principles for designing training interventions



Subject: Revision to Your Amazon.com Information

SquirrelMail 1.4.5

http://err.cylab.cmu.edu/mail/src/webmail.php

Most Visited | SquirrelMail 1.5.1 | EDAS Conference Ma... | Carnegie Mellon Dir... | APWG EMAILS FEATU... | Conference on Email...

Folders
Last Refresh:
Tue, 2:39 pm
(Check mail)

INBOX (1)
INBOX.Draft
INBOX.Sent
INBOX.Trash

Current Folder: **INBOX** Sign Out

Compose Addresses Folders Options Search Help SquirrelMail

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

Subject: Revision to Your Amazon.com Information

To: bsmith@cognix.com
Priority: Normal
Options: View Full Header | View Printable Version

amazon.com.

Please login and enter your information

Please follow this link to update your personal information:

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

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.

This message was generated automatically, please do not reply to it. Amazon treats your personal information with the utmost care, and our Privacy Policy is designed to protect you and your information.

Done

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.

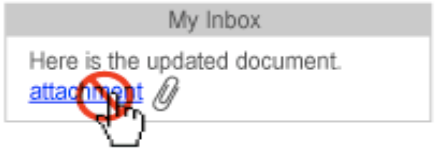
2. Never give out personal information upon email request.

3. Look carefully at the web address.

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

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.

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



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!

Laboratory study results

- Security notices are an ineffective medium for training users
- Users educated with embedded training make better decisions than those sent security notices
- Participants retained knowledge after 7 days
- Training does not increase false positive error

Real world study: Portuguese ISP

- PhishGuru is effective in training people in the real world
  - Statistically significant difference between Day 0 and Day 2 in both generic and spear conditions (p-value < 0.05)
- Trained participants retained knowledge after 7 days of training
  - No significant difference in generic or spear conditions between Day 2 and Day 7

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. Lessons from a real world evaluation of anti-phishing training. e-Crime Researchers Summit, 2008

CMU-PhishGuru study design and results

CMU study

- 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. 2009. *Under review.* http://www.cylab.cmu.edu/research/techreports/cmucylab09002.pdf

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)
- Counterbalanced emails and interventions
- 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
- Websites fully functional
- 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.

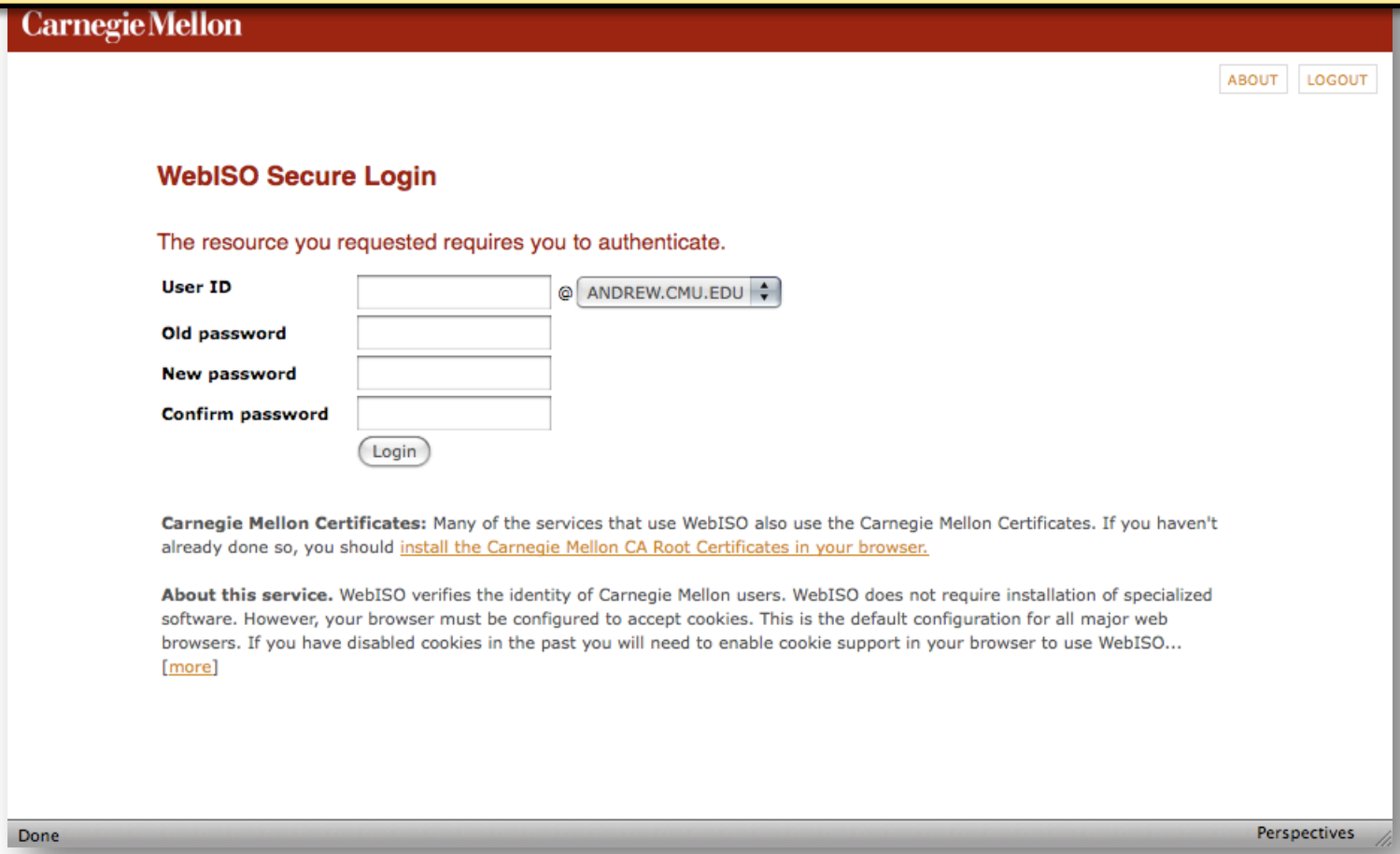
http://andrewwebmail.org/password/change.htm?ID=9009

URL is not hidden

Sincerely,
Andrew Help Desk

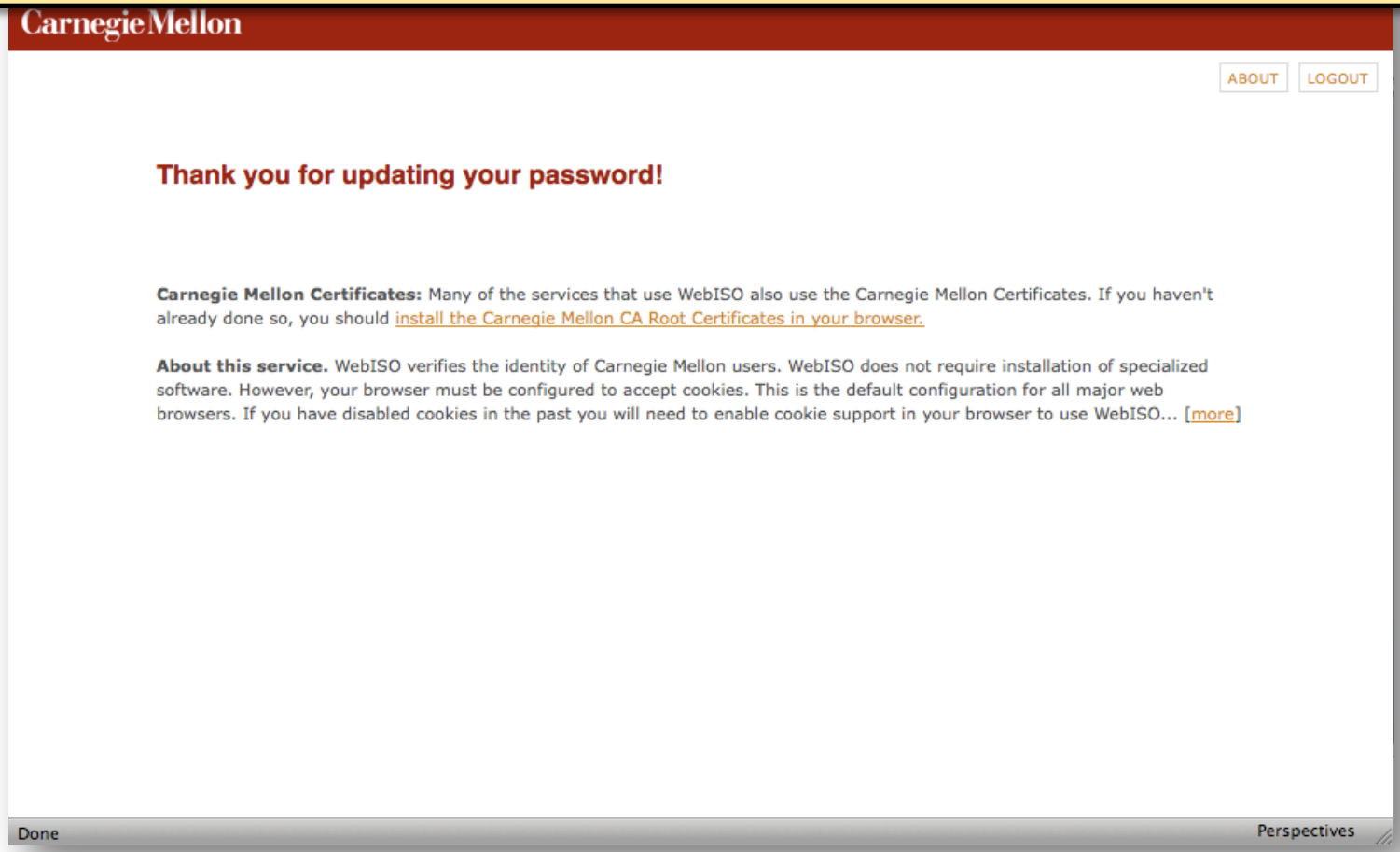
Simulated phishing website

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



Simulated phishing website

http://andrewwebmail.org/password/thankyou.html?ID=9009



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

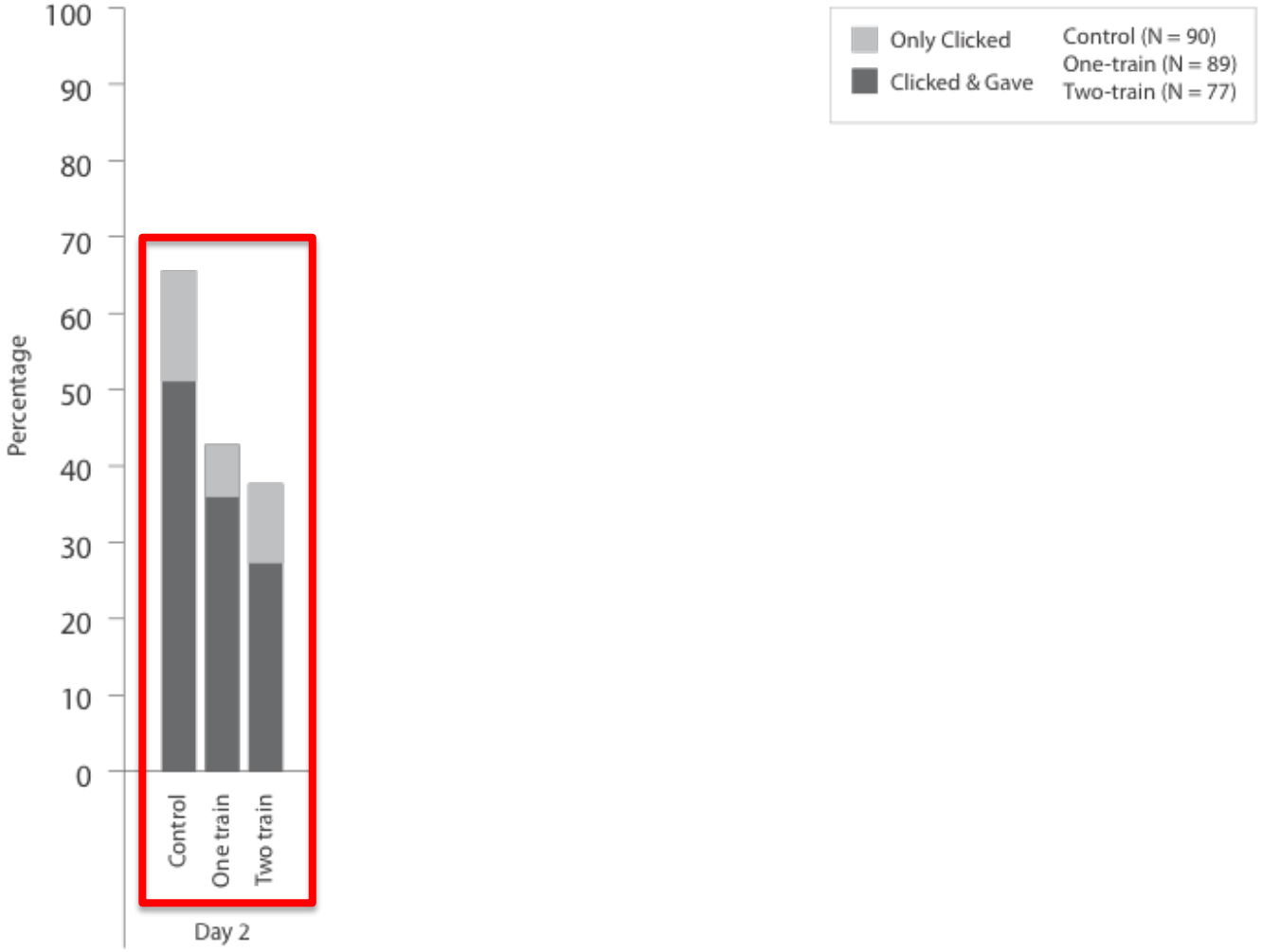
Results

- 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

Effect of PhishGuru

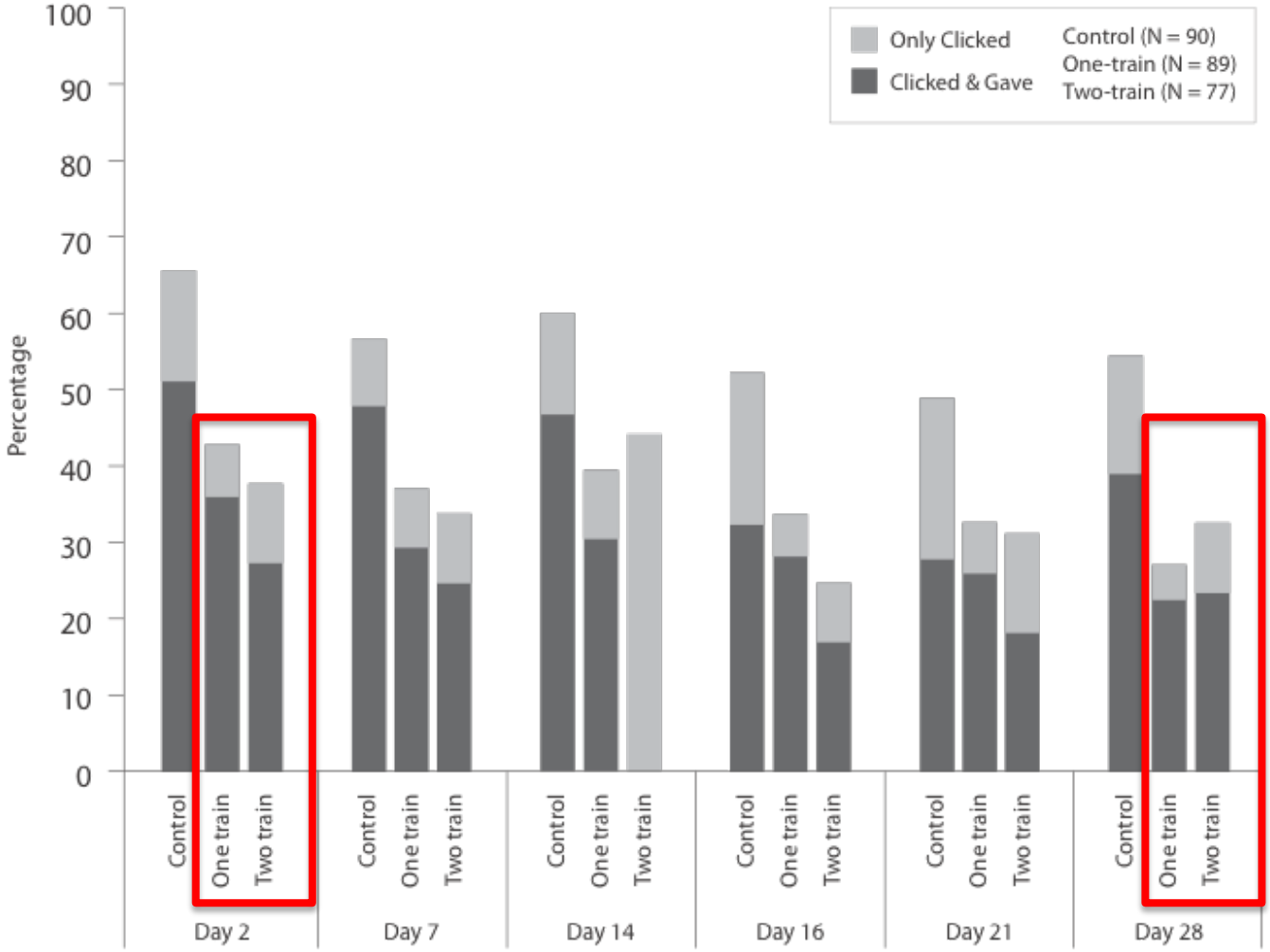
Condition	N	% who clicked on Day 0	% who clicked on Day 28
Control	172	52.3	44.2
Trained	343	48.4	24.5

Results conditioned on participants who clicked on day 0



Trained participants less likely to fall for phish

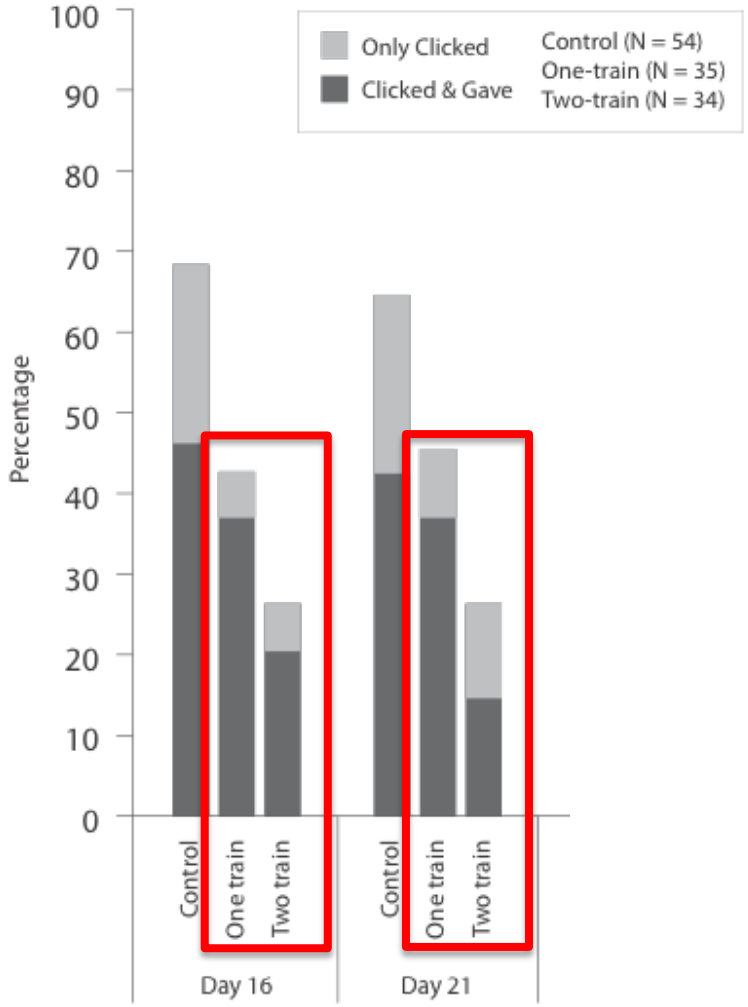
Results conditioned on participants who clicked on day 0



Trained participants less likely to fall for phish

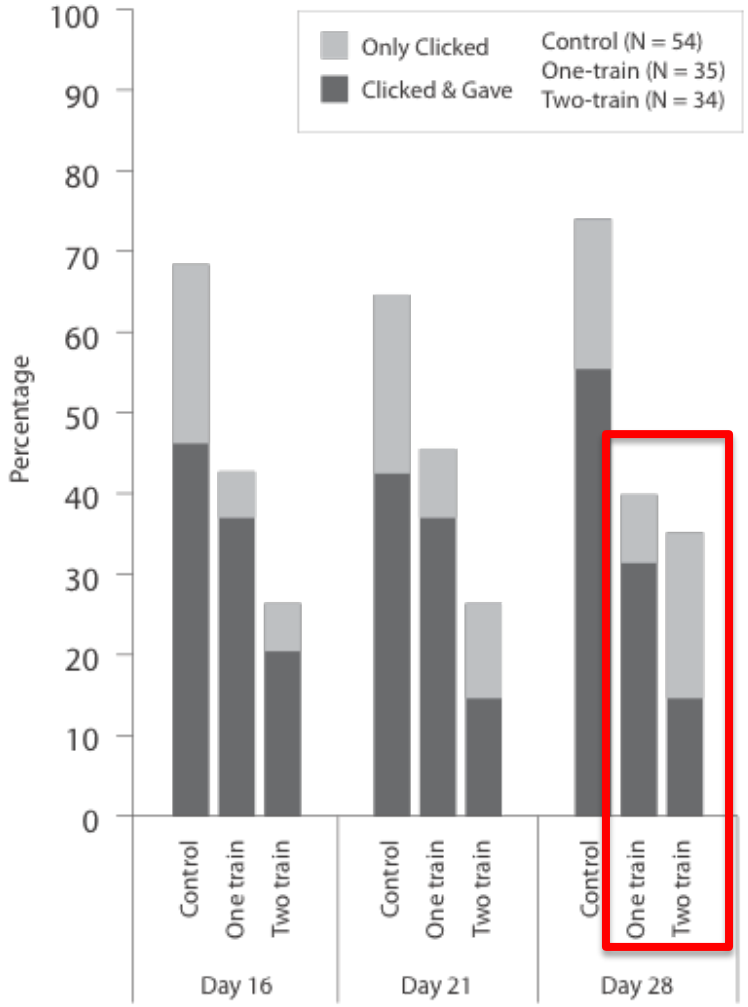
Trained participants remember what they learned 28 days later

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%

Inquiries received

- 263 inquiries to ISO/helpdesk
- Most of the users identified it as phish and reported about the email
- Some participants did not identify the emails as phish
  - Some of them attempted to follow the link

Personal emails received

- 39 emails to Lorrie/PK
  - Identifying the emails as phishing emails
  - Checking whether the emails were phishing
  - Thanking for teaching them to identify phishing emails
  - Other system administrators keep us in loop

Most participants liked training, wanted more

- 280 complete post study responses
- 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!"

Study conclusion

- Users retained knowledge even 28 days
- Users who saw the training intervention twice did better than those who saw the intervention once
- Users read the emails within 8 hours of the time the email was sent
- Younger users are more vulnerable to phishing than older users

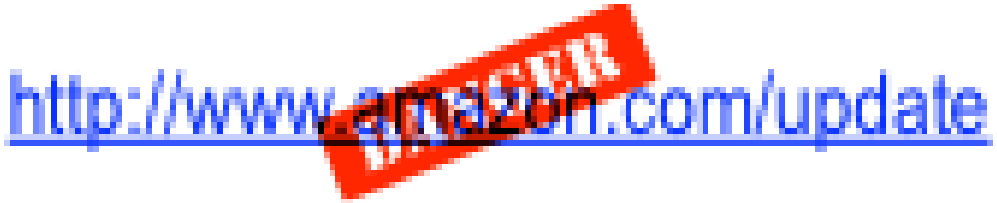
Research to reality

- PhishGuru commercialized
- Co-founded by faculty at CMU
  - Dr. Lorrie Cranor
  - Dr. Jason Hong
  - Dr. Norman Sadeh

wombat
security technologies

How to protect yourself

Don’t trust links in an email

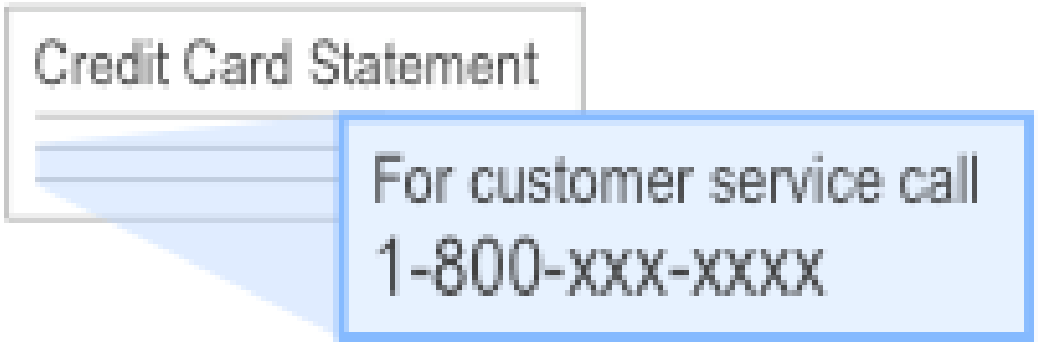


Never give out personal information upon email request

Look carefully at the web address

Type in the real website address into a web browser

Don’t call company phone numbers in emails or instant messages



Don’t open unexpected email attachments or instant message download links

Lessons learned

Lessons learned (on community)

- The community is very supportive
- The ISO didn't undermine its community standing
- There are more helpers than help centers
- We've got some detectives in our midst
- Some people are more behind on their email than me

Lessons learned (on phishing)

- Age matters
- Layered defenses are important but **the end-user is still the final defender** and they can be duped into divulging their credentials by a well-crafted phishing attack
- Just-in-time training and awareness
  - Make it 'useable': timely, relevant, unavoidable, and fun
- Lather, rinse, repeat

Lessons learned (on research)

- Answering one question leads to two more
- Research is real work, partnership makes it fun

Acknowledgements

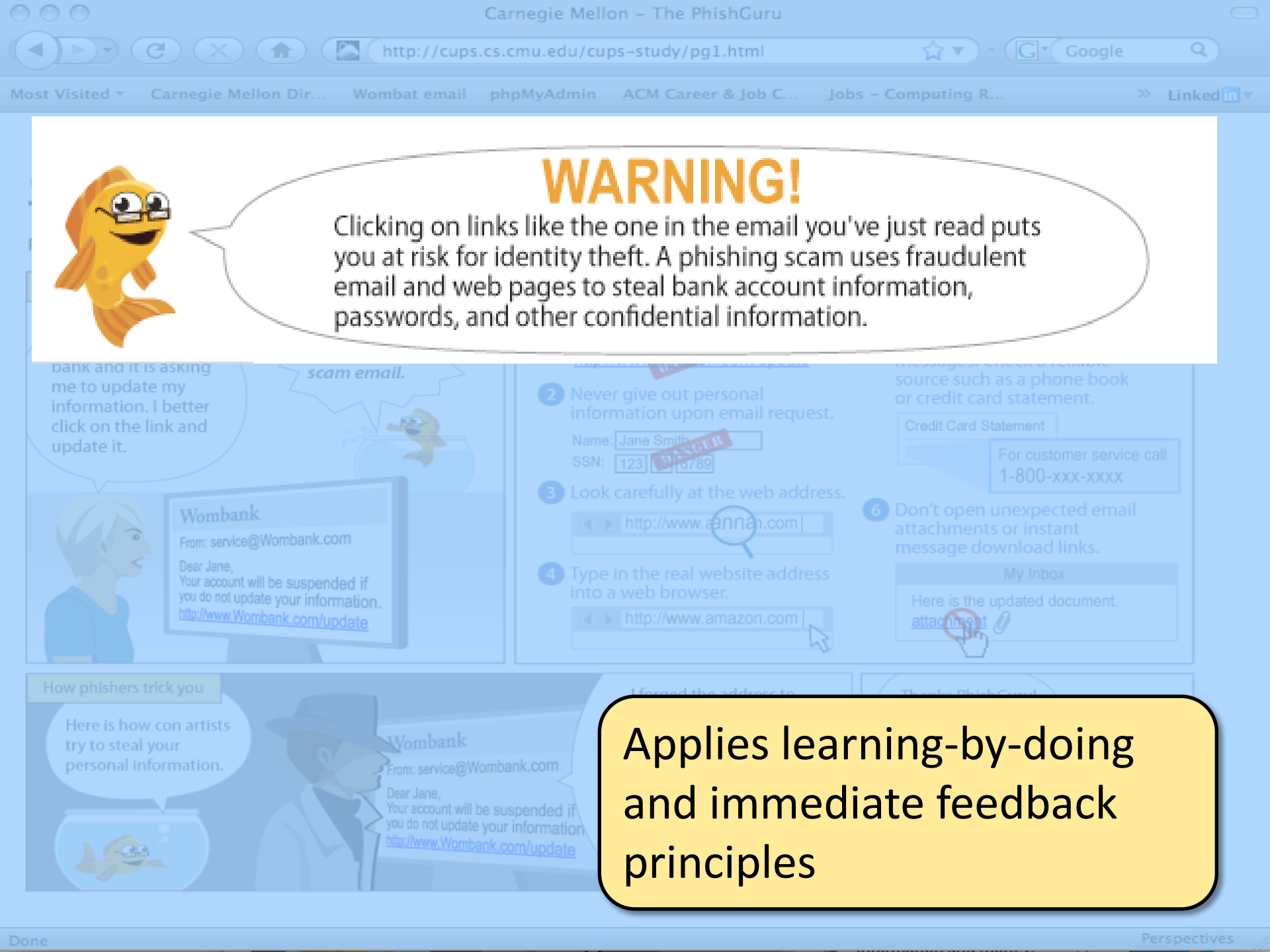
- All participants
- System administrators around the campus
- Campus Help Centers
- Departments that we spoofed
- Members of CUPS

CyLab Usable Privacy and Security Laboratory

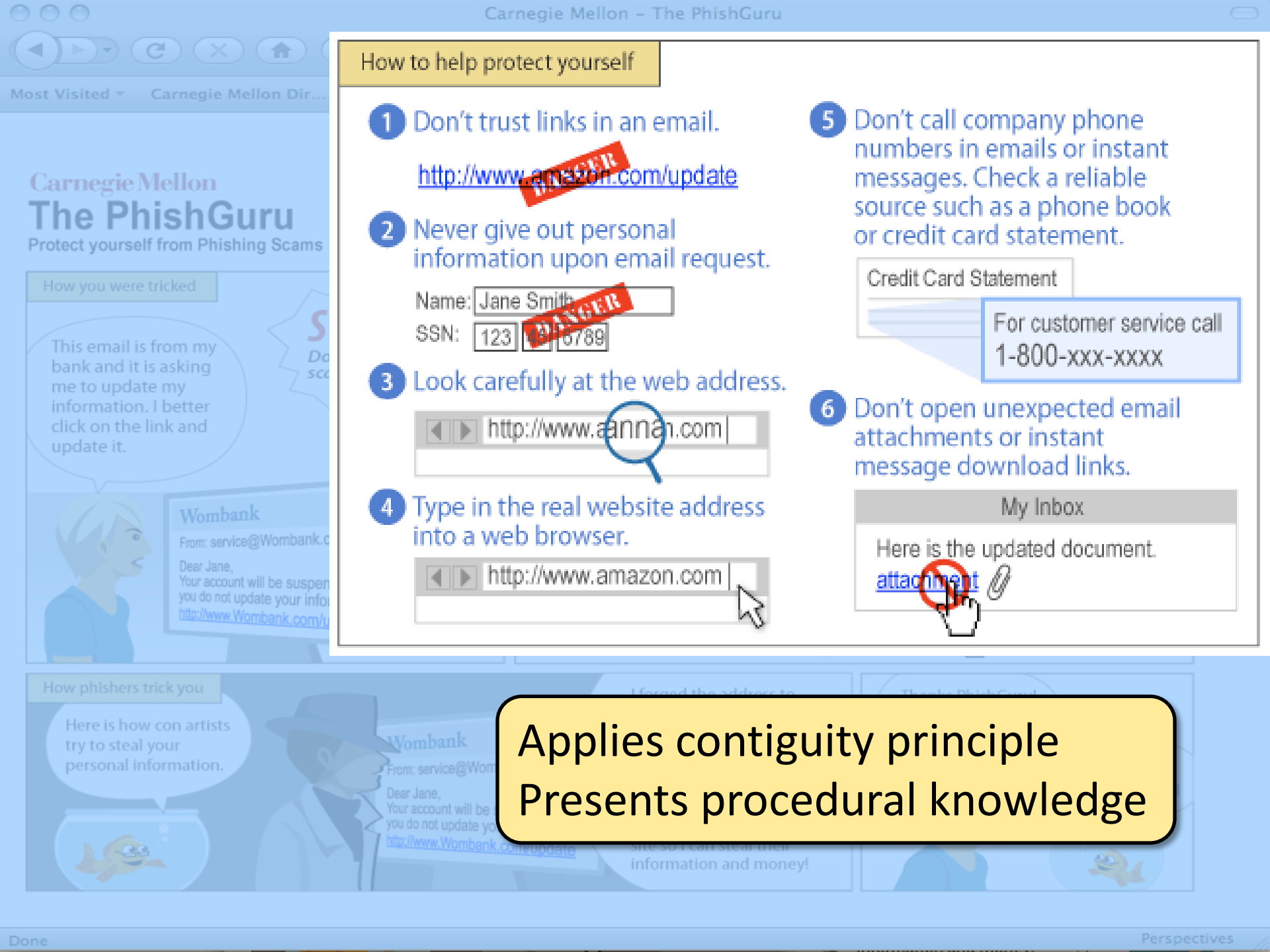
http://www.cups.cs.cmu.edu/

http://phishguru.org/

Backup slides


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.anna.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.
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


Carnegie Mellon – The PhishGuru
Most Visited
Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams
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.
Wombank
From: service@Wombank.c
Dear Jane,
Your account will be suspen
you do not update your info
http://www.Wombank.com/u
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 45 6789
DANGER
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.
Wombank
From: service@Wom
Dear Jane,
Your account will be
you do not update yo
http://www.Wombank.com/update
information and money!
Applies contiguity principle
Presents procedural knowledge
Done
Perspectives

Carnegie Mellon – The PhishGuru

http://cups.cs.cmu.edu/cups-study/pg1.html

Most Visited | Carnegie Mellon Dir... | Wombat email | phpMyAdmin | ACM Career & Job C... | Jobs – Computing R...

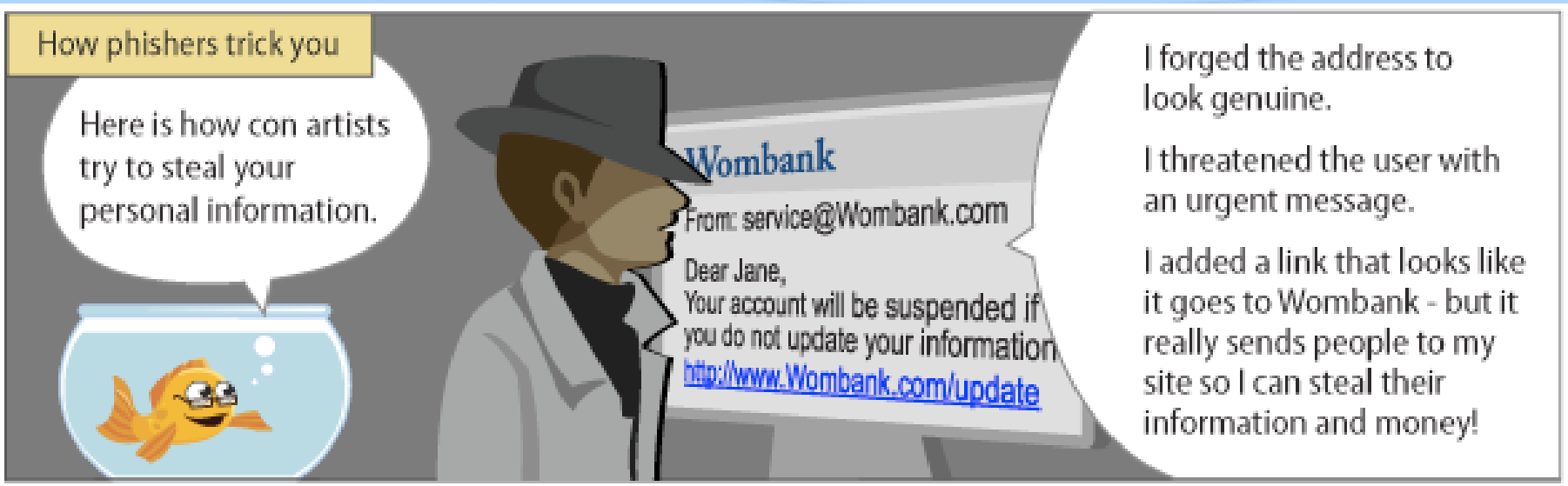
Carnegie Mellon

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.

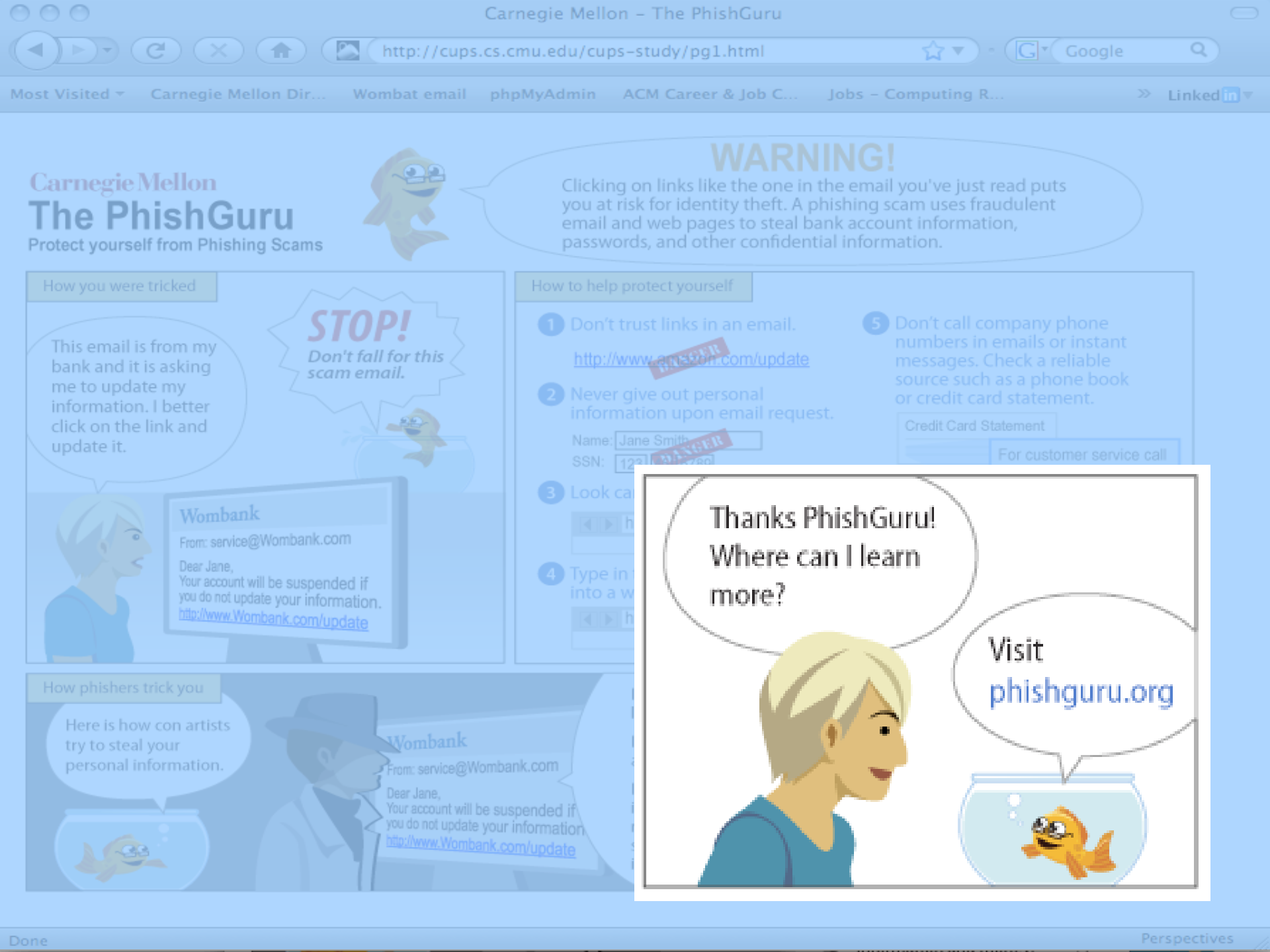


Applies personalization principle

Presents conceptual knowledge

Done

Perspectives


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:
3 Look ca
4 Type in
into a w
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

Phishing

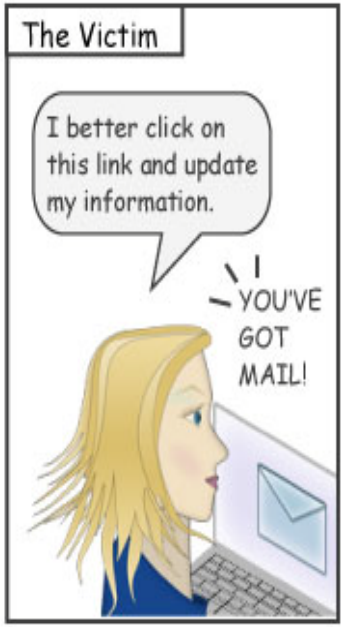
Clicking on links like the one in the email you've just read puts you at risk for identity theft and financial loss. Such emails are called phishing scams.

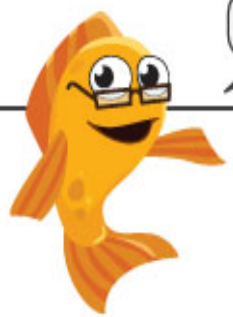
I **forged** the address to look **genuine**.

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

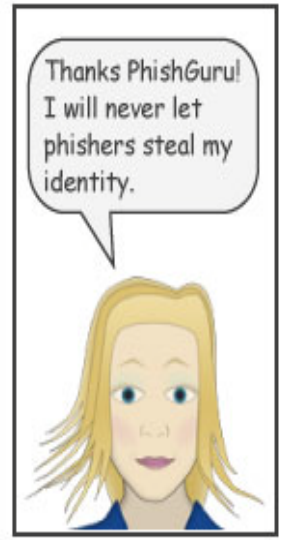
I added a link that looks like it goes to a book store, but really it sends people to my site so I can steal their information !

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.
   http://amazon.com
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.

How to help protect yourself

1. Don't trust links in an email.

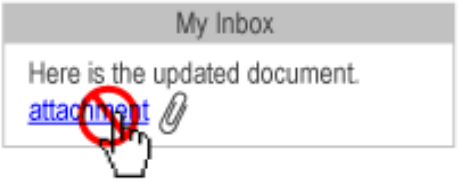
2. Never give out personal information upon email request.

3. Look carefully at the web address.

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

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.

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



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

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.

Do you know any time an email asks you to take an urgent action and type in your account number or social security number, it is probably a scam?

Really? How do I protect myself from these scams?

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 DANGER
   SSN: 123 [redacted] 6789

3. Look carefully at the web address.

   http://www.aanna.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. Where can I learn more?

Visit phishguru.org