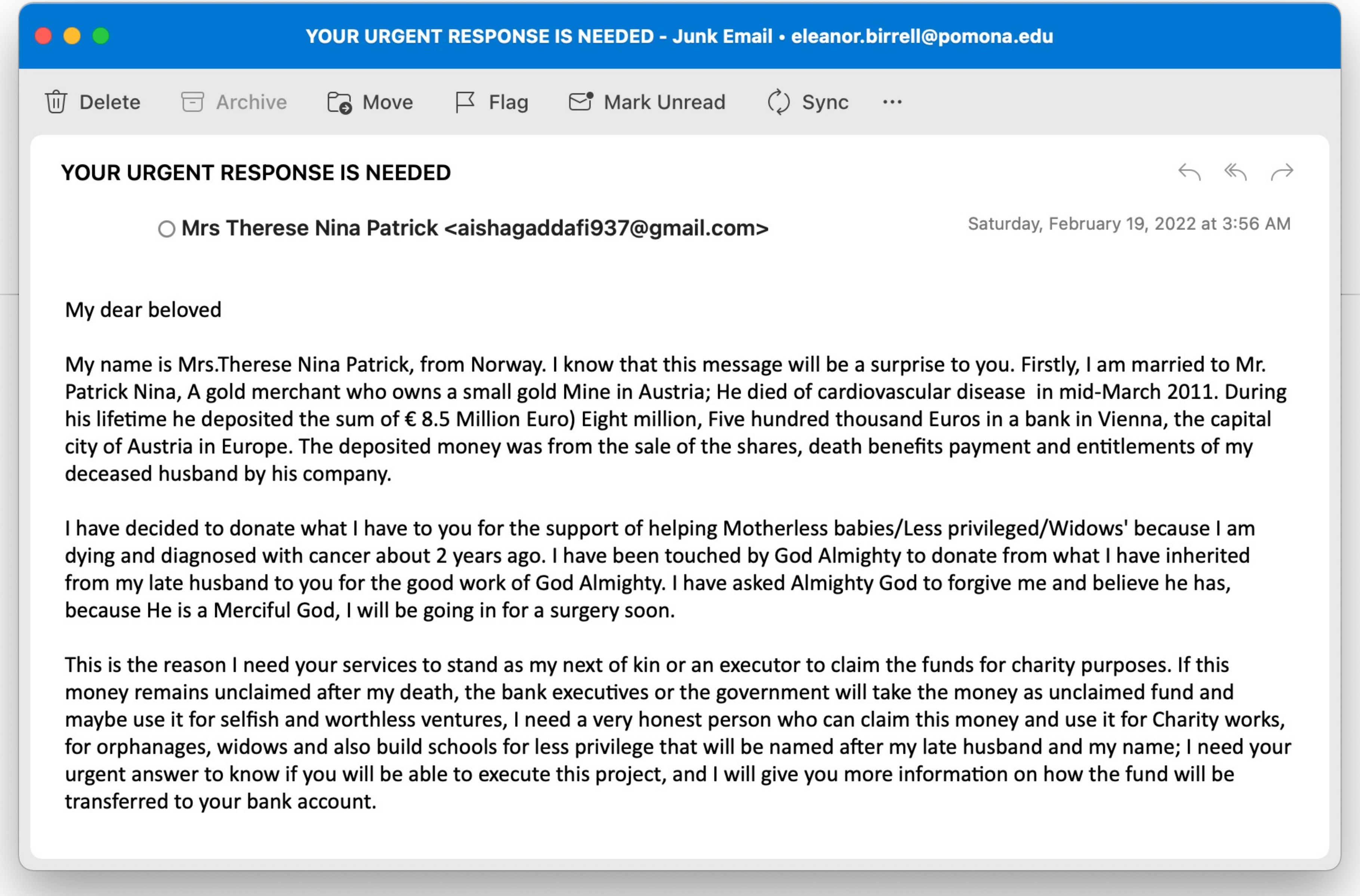
Lecture 15: Phishing Prevention

CS 181W

Fall 2022



YOUR URGENT RESPONSE IS NEEDED - Junk Email • eleanor.birrell@pomona.edu
Delete
Archive
Move
Flag
Mark Unread
Sync
···

YOUR URGENT RESPONSE IS NEEDED

○ Mrs Therese Nina Patrick <aishagaddafi937@gmail.com>

Saturday, February 19, 2022 at 3:56 AM

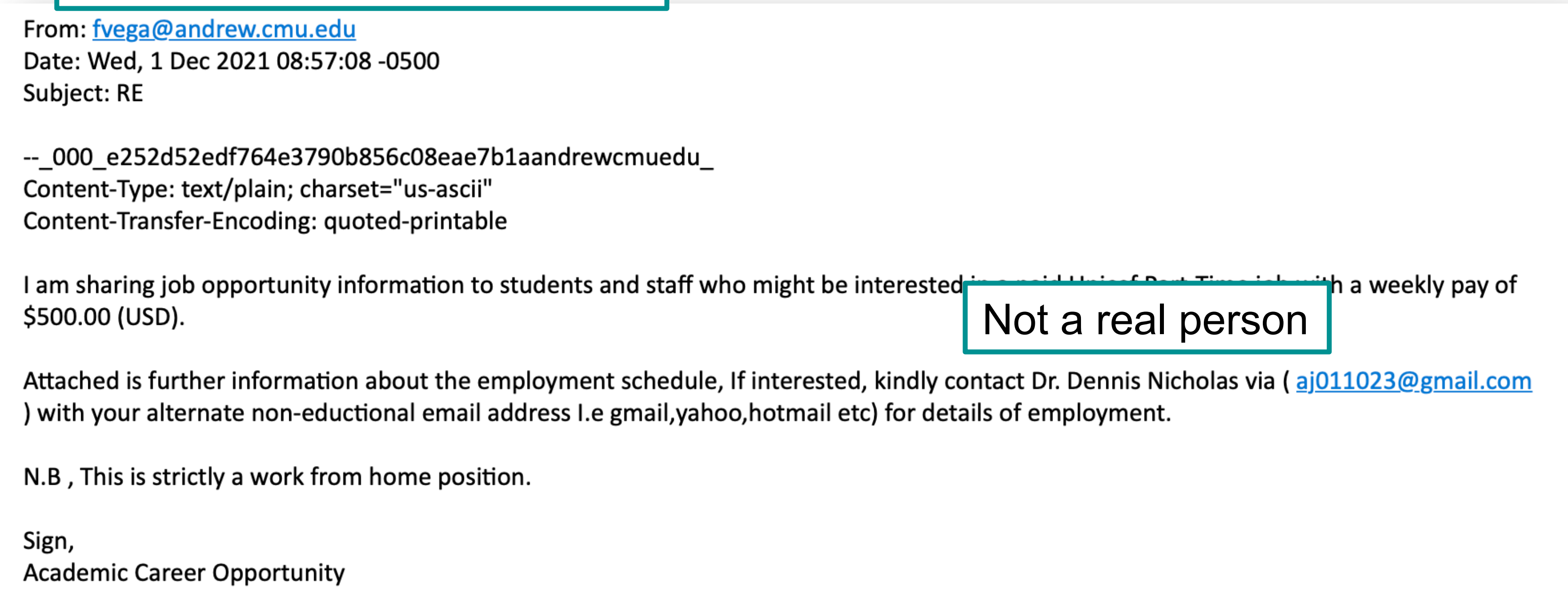
My dear beloved

My name is Mrs.Therese Nina Patrick, from Norway. I know that this message will be a surprise to you. Firstly, I am married to Mr. Patrick Nina, A gold merchant who owns a small gold Mine in Austria; He died of cardiovascular disease in mid-March 2011. During his lifetime he deposited the sum of € 8.5 Million Euro) Eight million, Five hundred thousand Euros in a bank in Vienna, the capital city of Austria in Europe. The deposited money was from the sale of the shares, death benefits payment and entitlements of my deceased husband by his company.

I have decided to donate what I have to you for the support of helping Motherless babies/Less privileged/Widows' because I am dying and diagnosed with cancer about 2 years ago. I have been touched by God Almighty to donate from what I have inherited from my late husband to you for the good work of God Almighty. I have asked Almighty God to forgive me and believe he has, because He is a Merciful God, I will be going in for a surgery soon.

This is the reason I need your services to stand as my next of kin or an executor to claim the funds for charity purposes. If this money remains unclaimed after my death, the bank executives or the government will take the money as unclaimed fund and maybe use it for selfish and worthless ventures, I need a very honest person who can claim this money and use it for Charity works, for orphanages, widows and also build schools for less privilege that will be named after my late husband and my name; I need your urgent answer to know if you will be able to execute this project, and I will give you more information on how the fund will be transferred to your bank account.

Not a real CMU email address



From: fvega@andrew.cmu.edu
Date: Wed, 1 Dec 2021 08:57:08 -0500
Subject: RE

--_000_e252d52edf764e3790b856c08eae7b1aandrewcmuedu_
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

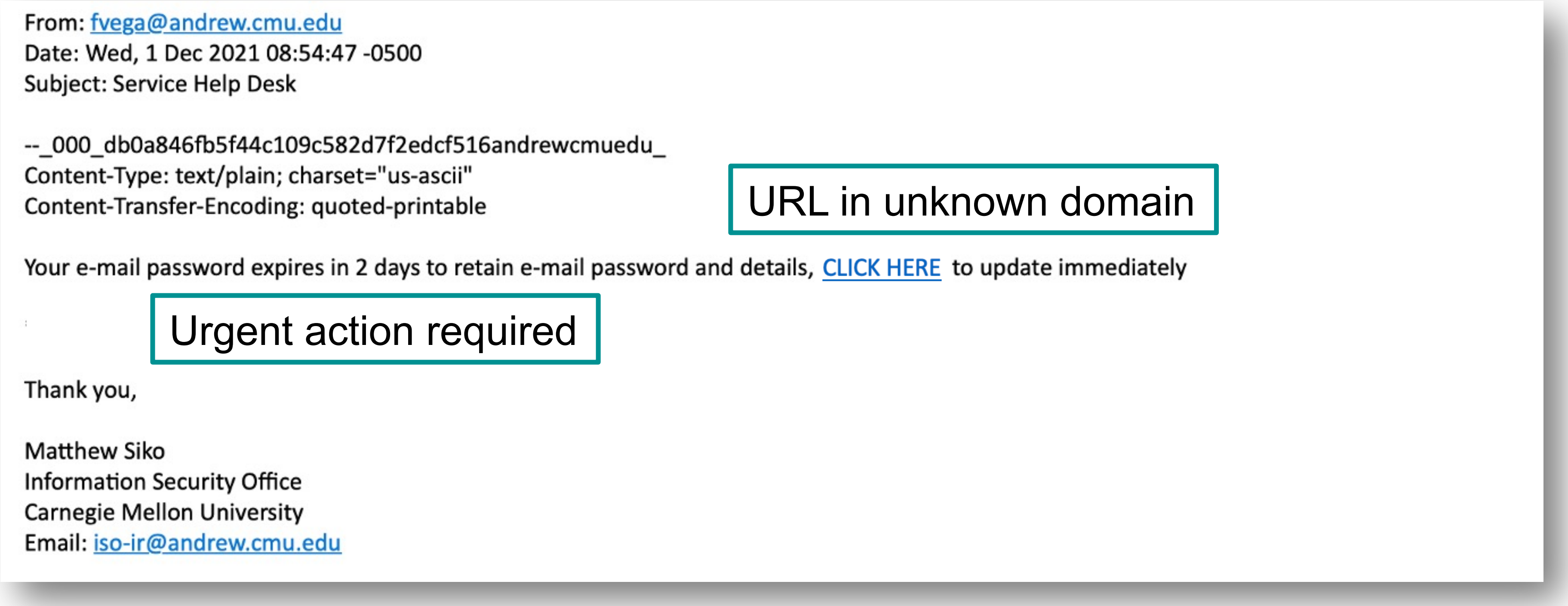
I am sharing job opportunity information to students and staff who might be interested in a paid Unicef Part Time job with a weekly pay of $500.00 (USD).

Not a real person

Attached is further information about the employment schedule, If interested, kindly contact Dr. Dennis Nicholas via (aj011023@gmail.com) with your alternate non-eductional email address I.e gmail,yahoo,hotmail etc) for details of employment.

N.B , This is strictly a work from home position.

Sign,
Academic Career Opportunity



From: fvega@andrew.cmu.edu
Date: Wed, 1 Dec 2021 08:54:47 -0500
Subject: Service Help Desk

--_000_db0a846fb5f44c109c582d7f2edcf516andrewcmuedu_
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

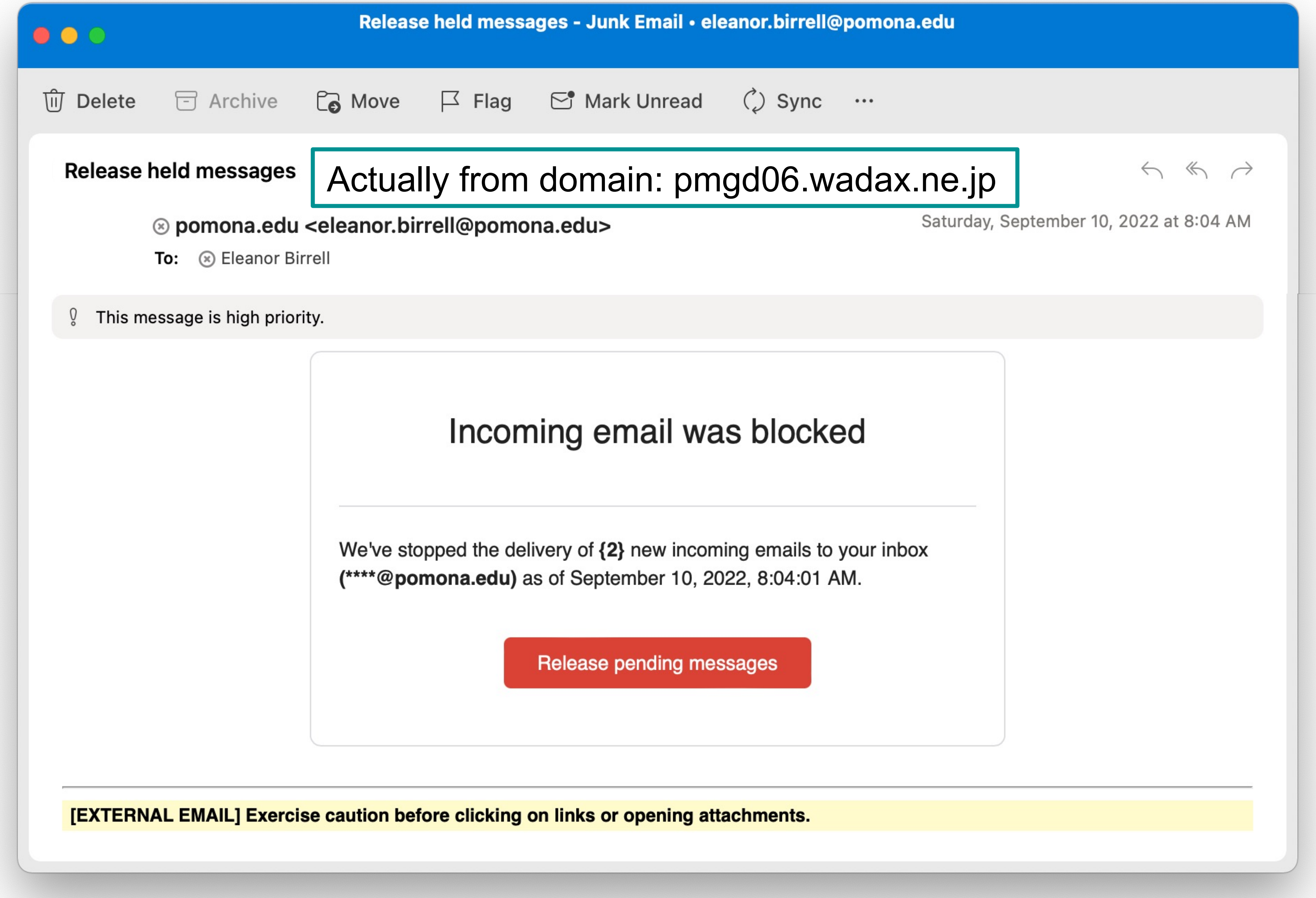
URL in unknown domain

Your e-mail password expires in 2 days to retain e-mail password and details, CLICK HERE to update immediately

Urgent action required

Thank you,

Matthew Siko
Information Security Office
Carnegie Mellon University
Email: iso-ir@andrew.cmu.edu



Release held messages - Junk Email • eleanor.birrell@pomona.edu

Release held messages

Actually from domain: pmgd06.wadax.ne.jp

pomona.edu <eleanor.birrell@pomona.edu>

Saturday, September 10, 2022 at 8:04 AM

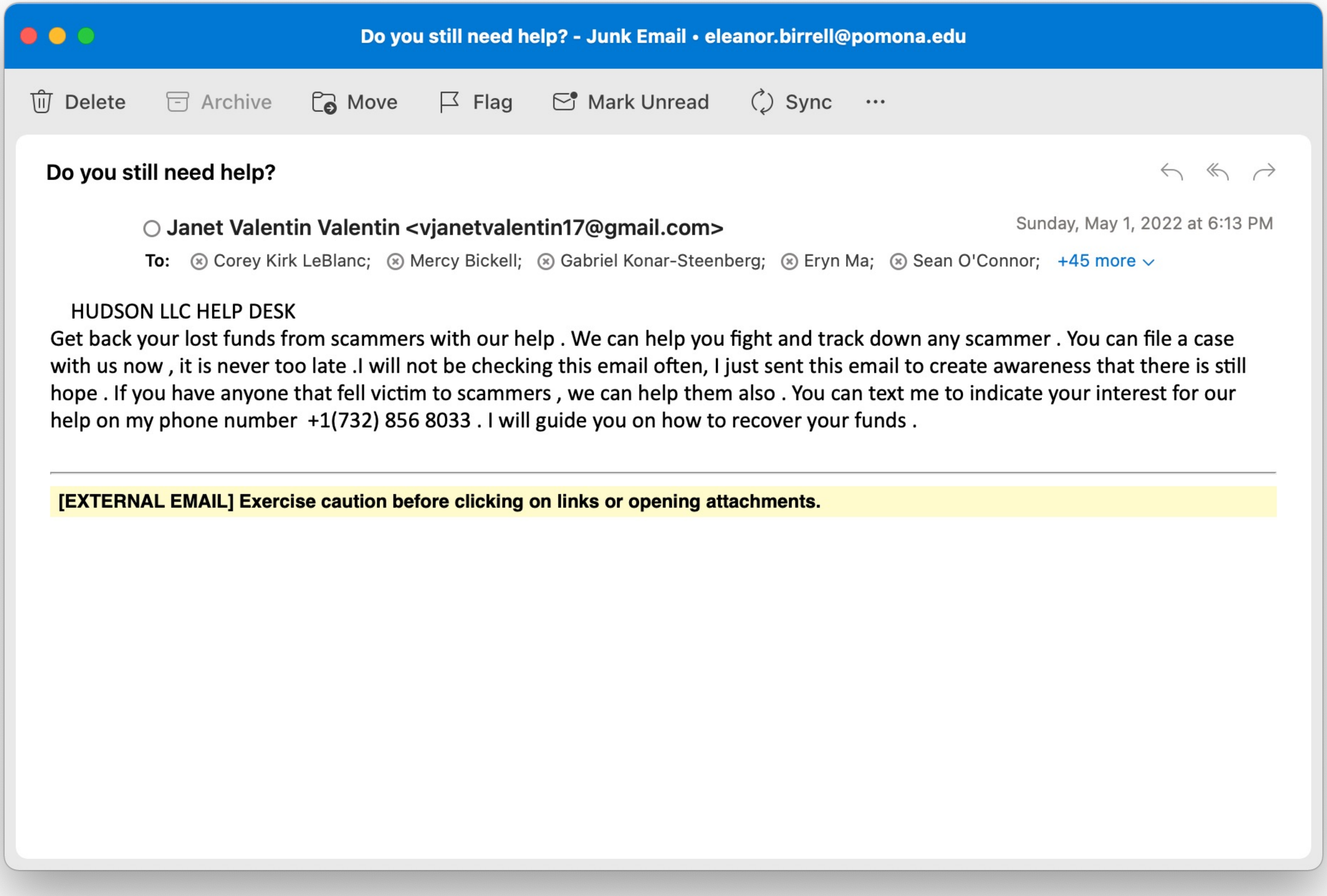
To: Eleanor Birrell

This message is high priority.

Incoming email was blocked

We've stopped the delivery of **{2}** new incoming emails to your inbox **(****@pomona.edu)** as of September 10, 2022, 8:04:01 AM.

[EXTERNAL EMAIL] Exercise caution before clicking on links or opening attachments.


Do you still need help? - Junk Email • eleanor.birrell@pomona.edu
Delete
Archive
Move
Flag
Mark Unread
Sync
···

Do you still need help?

○ Janet Valentin Valentin <vjanetvalentin17@gmail.com>

Sunday, May 1, 2022 at 6:13 PM

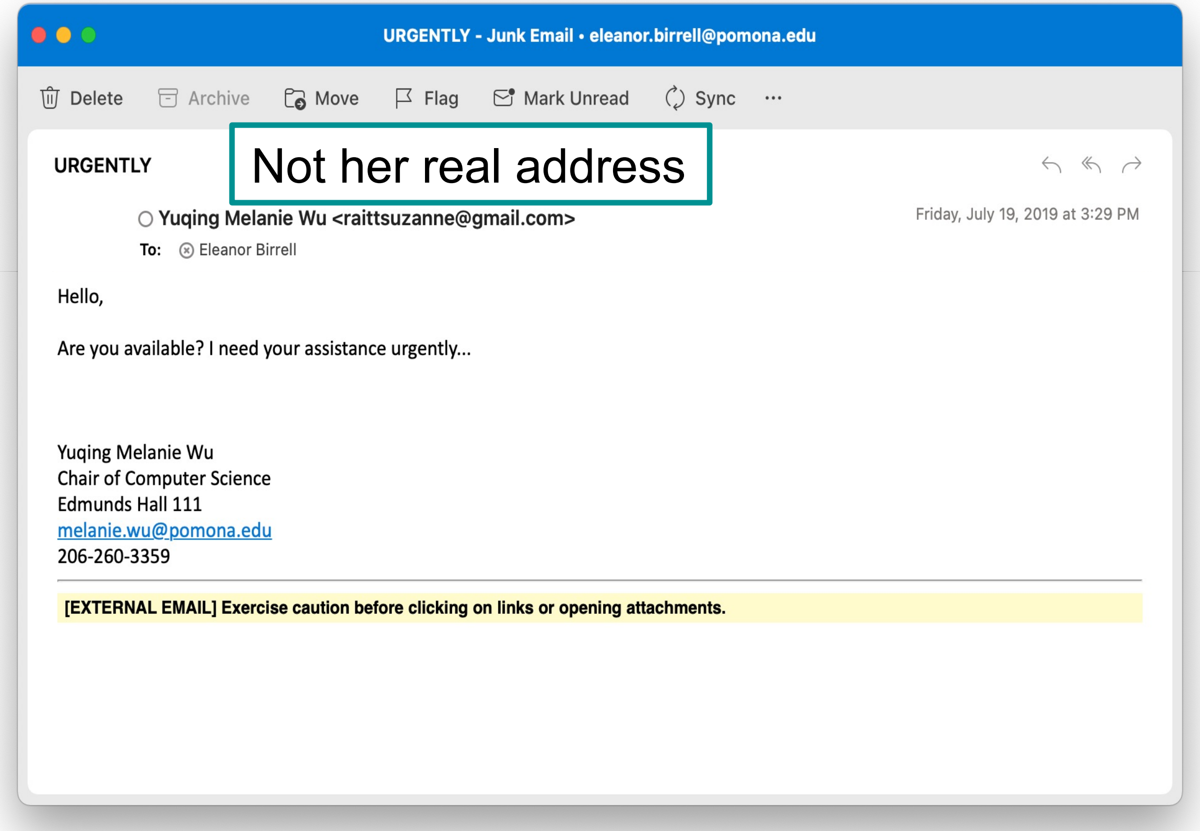
To: ⊗ Corey Kirk LeBlanc; ⊗ Mercy Bickell; ⊗ Gabriel Konar-Steenberg; ⊗ Eryn Ma; ⊗ Sean O'Connor; +45 more

HUDSON LLC HELP DESK
Get back your lost funds from scammers with our help . We can help you fight and track down any scammer . You can file a case with us now , it is never too late .I will not be checking this email often, I just sent this email to create awareness that there is still hope . If you have anyone that fell victim to scammers , we can help them also . You can text me to indicate your interest for our help on my phone number +1(732) 856 8033 . I will guide you on how to recover your funds .

[EXTERNAL EMAIL] Exercise caution before clicking on links or opening attachments.

Spear phishing

- Targets specific groups of individuals
- Often targeted towards an organization’s employees rather than their customers



Not her real address

URGENTLY

○ Yuqing Melanie Wu <raittsuzanne@gmail.com>

To: Eleanor Birrell

Friday, July 19, 2019 at 3:29 PM

Hello,

Are you available? I need your assistance urgently...

Yuqing Melanie Wu
Chair of Computer Science
Edmunds Hall 111
melanie.wu@pomona.edu
206-260-3359

[EXTERNAL EMAIL] Exercise caution before clicking on links or opening attachments.

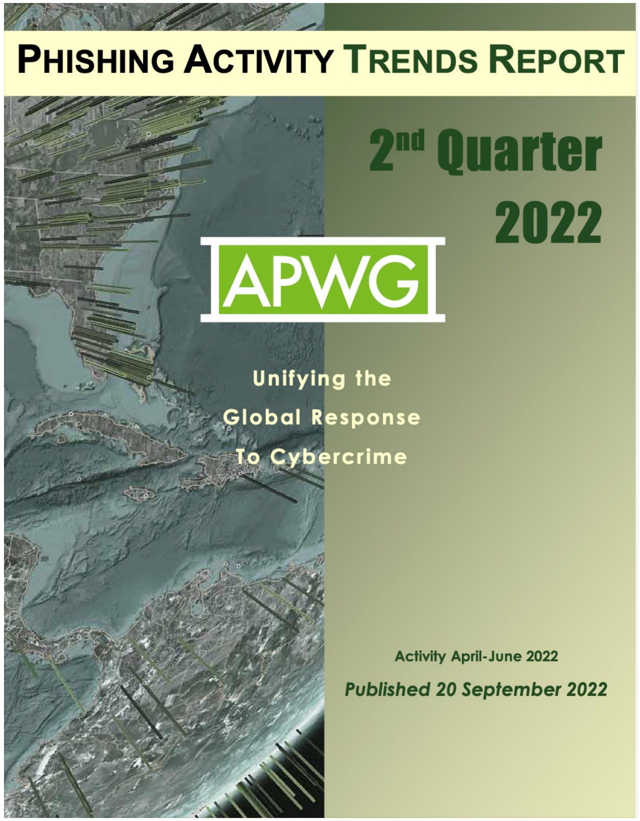
High volume of phishing attacks

- 76% of businesses reported being a victim of a phishing attack in 2017 [Wombat Security State of the Phish]
- 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link [Verizon Data Breach Investigations Report]
- 95% of all attacks on enterprise networks are the result of successful spear phishing [SANS Institute]
- Nearly 1.5 million new phishing sites are created each month [Webroot Threat Report]

Eitan Katz. Phishing statistics: what every business needs to know. Dashlane blog. January 17, 2018 .
https://blog.dashlane.com/phishing-statistics/

2022 trends summary

- Phishing attacks are at an all-time high (more than tripled since early 2020)
- 40% of phishing cash-out with gift cards
- Most targeted industries: financial institutions, webmail providers, social media
- Average wire transfer request in business email compromise scams: $109,467



PHISHING ACTIVITY TRENDS REPORT

2nd Quarter 2022

APWG

Unifying the Global Response To Cybercrime

Activity April-June 2022

Published 20 September 2022

Why phishing works

- Phishers take advantage of Internet users’ trust in legitimate organizations
- Lack of computer and security knowledge
- People don’t use good strategies to protect themselves

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

- Recover from attacks quickly

- 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?

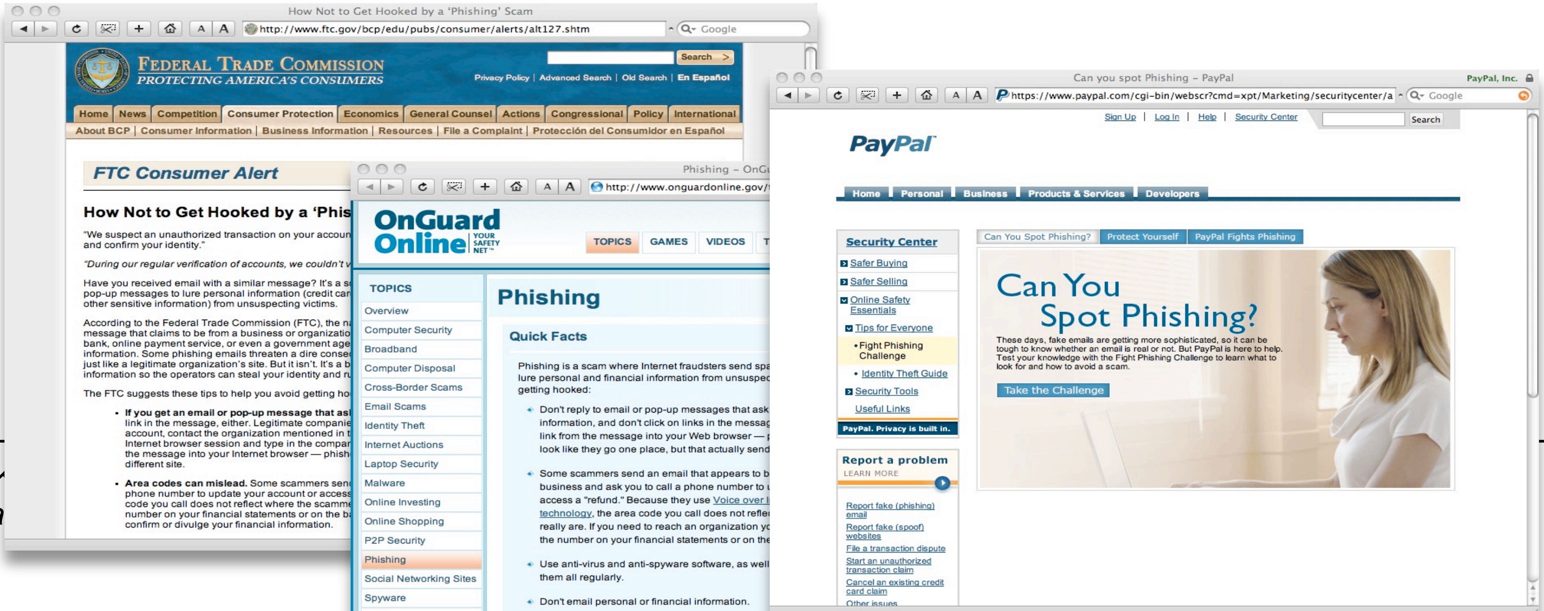
- Security education “puts the burden on the wrong shoulder.”
  [Nielsen, J. 2004. User education is not the answer to security problems. http://www.useit.com/alertbox/20041025.html.]

- “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]

Web site training evaluation study

- Laboratory study of 28 non-expert computer users
- Experimental study: 2 conditions
  - **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



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 'Phis

"We suspect an unauthorized transaction on your accoun
and confirm your identity."

"During our regular verification of accounts, we couldn't v

Have you received email with a similar message? It's a s
pop-up messages to lure personal information (credit car
other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the na
message that claims to be from a business or organizatio
bank, online payment service, or even a government age
information. Some phishing emails threaten a dire conse
just like a legitimate organization's site. But it isn't. It's a b
information so the operators can steal your identity and ru

The FTC suggests these tips to help you avoid getting ho

- **If you get an email or pop-up message that as** link in the message, either. Legitimate companie account, contact the organization mentioned in t Internet browser session and type in the compar the message into your Internet browser — phish different site.
- **Area codes can mislead.** Some scammers sen phone number to update your account or access code you call does not reflect where the scamme number on your financial statements or on the ba confirm or divulge your financial information.

Phishing

Quick Facts

Phishing is a scam where Internet fraudsters send spa
lure personal and financial information from unsuspec
getting hooked:

- Don't reply to email or pop-up messages that ask information, and don't click on links in the messag link from the message into your Web browser — p look like they go one place, but that actually send
- Some scammers send an email that appears to b business and ask you to call a phone number to u access a "refund." Because they use Voice over I technology, the area code you call does not refle really are. If you need to reach an organization yo the number on your financial statements or on the
- Use anti-virus and anti-spyware software, as well them all regularly.
- Don't email personal or financial information.

Can you spot Phishing – PayPal
PayPal, Inc.
https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/a
Google
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.

P. K
Tra

Web site training evaluation study

- Laboratory study of 28 non-expert computer users
- Experimental study: 2 conditions
  - **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 learn from online training, if only they pay attention!

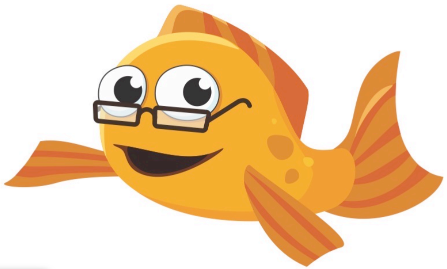
P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), May 2010.

How do we get people trained?

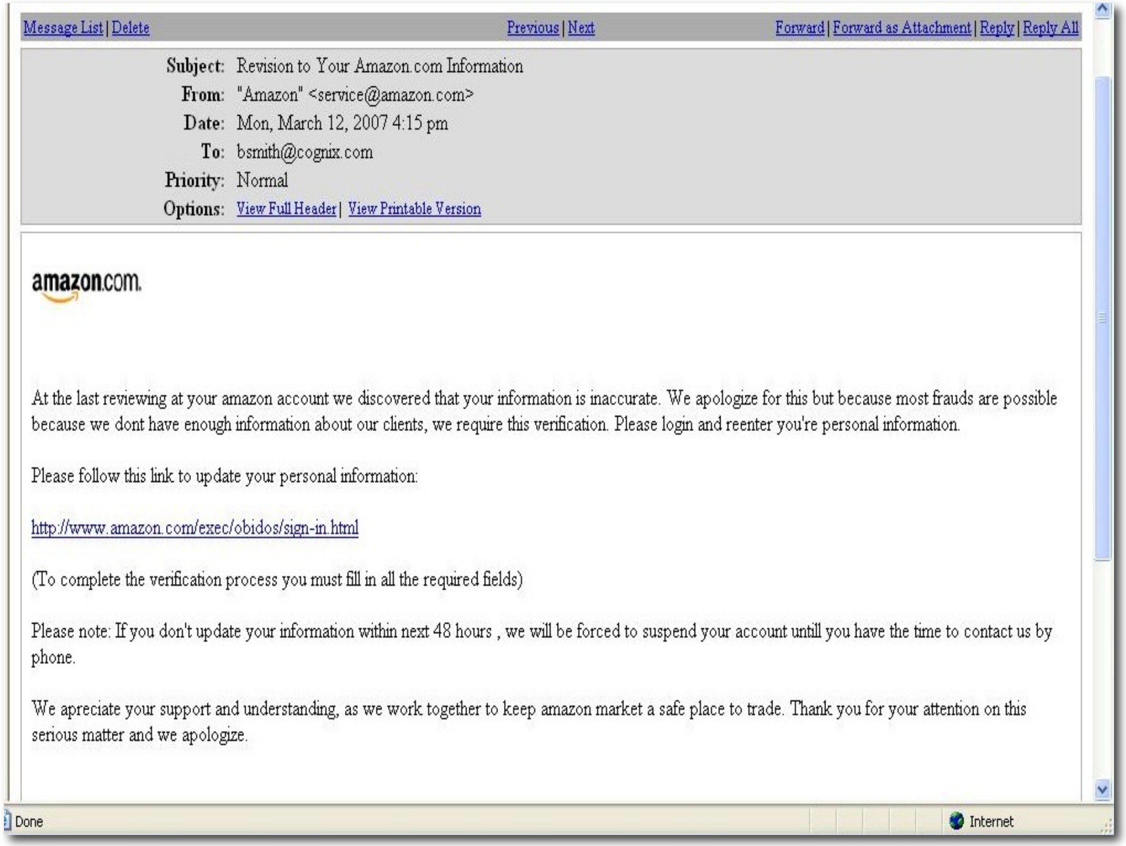
- Problem
  - Most people don’t proactively look for security training materials
  - “Security notice” emails sent to employees and/or customers tend to be ignored
    - Too much to read
    - People don’t consider them relevant
  - Existing (2010) materials good, but could be better

- Solution
  - Use learning science principles
  - Find a “teachable moment”: PhishGuru
  - Make training fun: Anti-Phishing Phil

PhishGuru embedded training



1. Send emails that looks like a phishing attack



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
Options: View Full Header | View Printable Version

amazon.com

At the last reviewing at your amazon account we discovered that your information is inaccurate. We apologize for this but because most frauds are possible because we dont have enough information about our clients, we require this verification. Please login and reenter you're personal information.

Please follow this link to update your personal information:

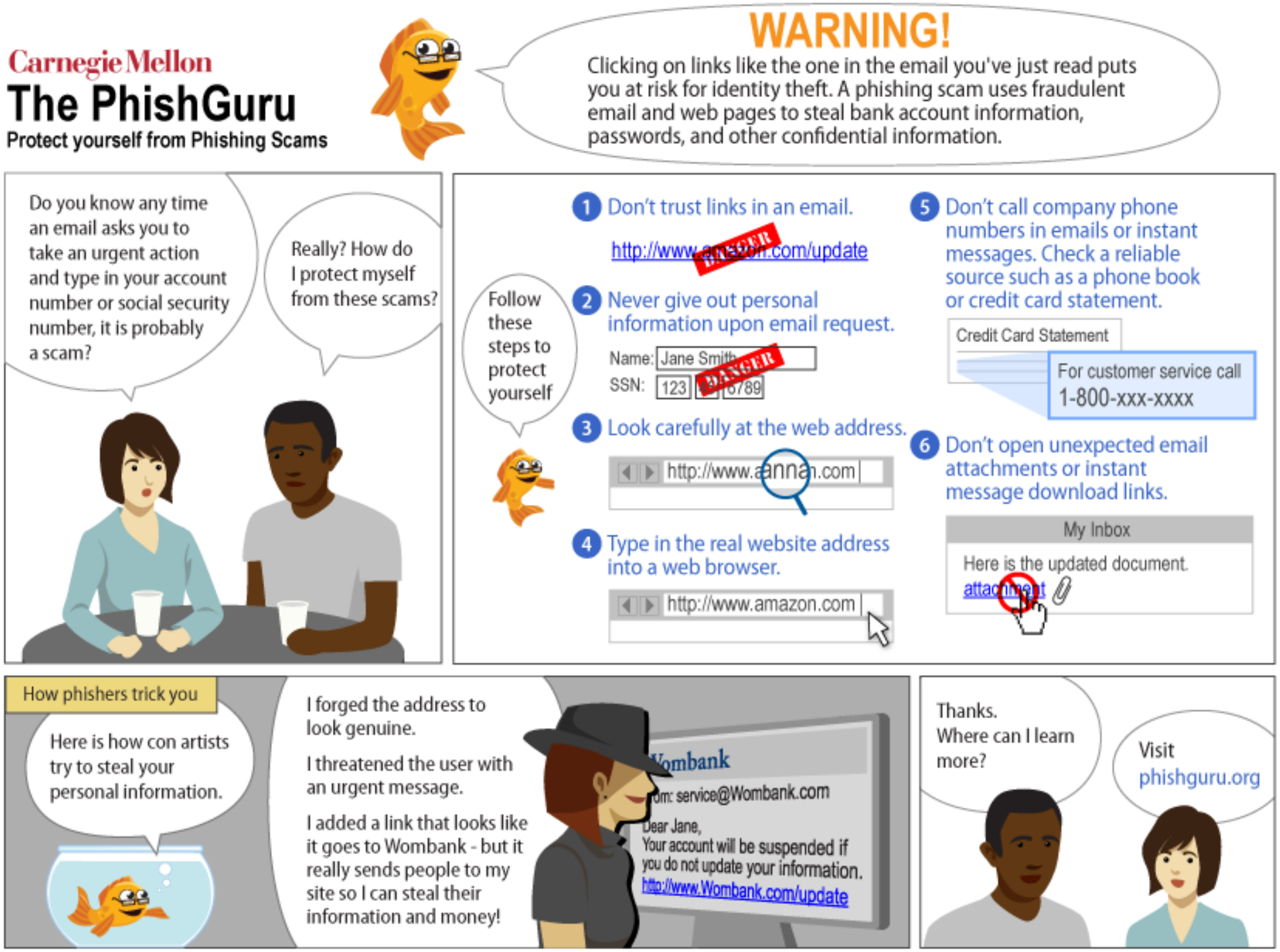
http://www.amazon.com/exec/obidos/sign-in.html

(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.

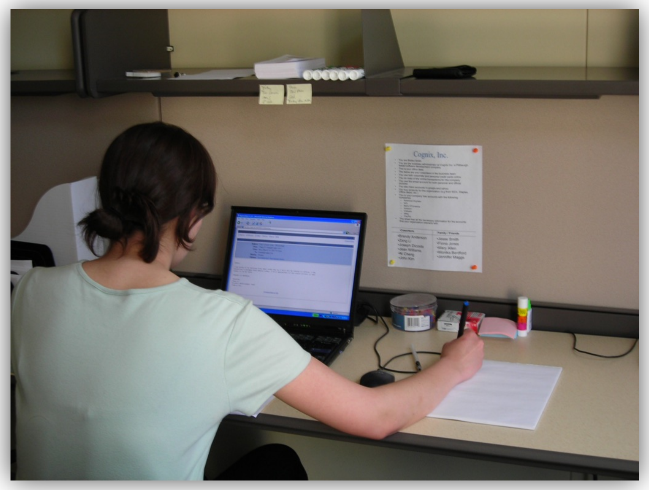
2. If recipient falls for it, intervention warns and highlights what cues to look for in succinct and engaging format


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
SSN: 123 6789
DANGER
3 Look carefully at the web address.
http://www.amannan.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!
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. Where can I learn more?
Visit phishguru.org

- Presents conceptual knowledge
- Presents procedural knowledge
- Applies story-based agent principle
- Applies learning-by-doing and immediate feedback principles

User Study

- 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

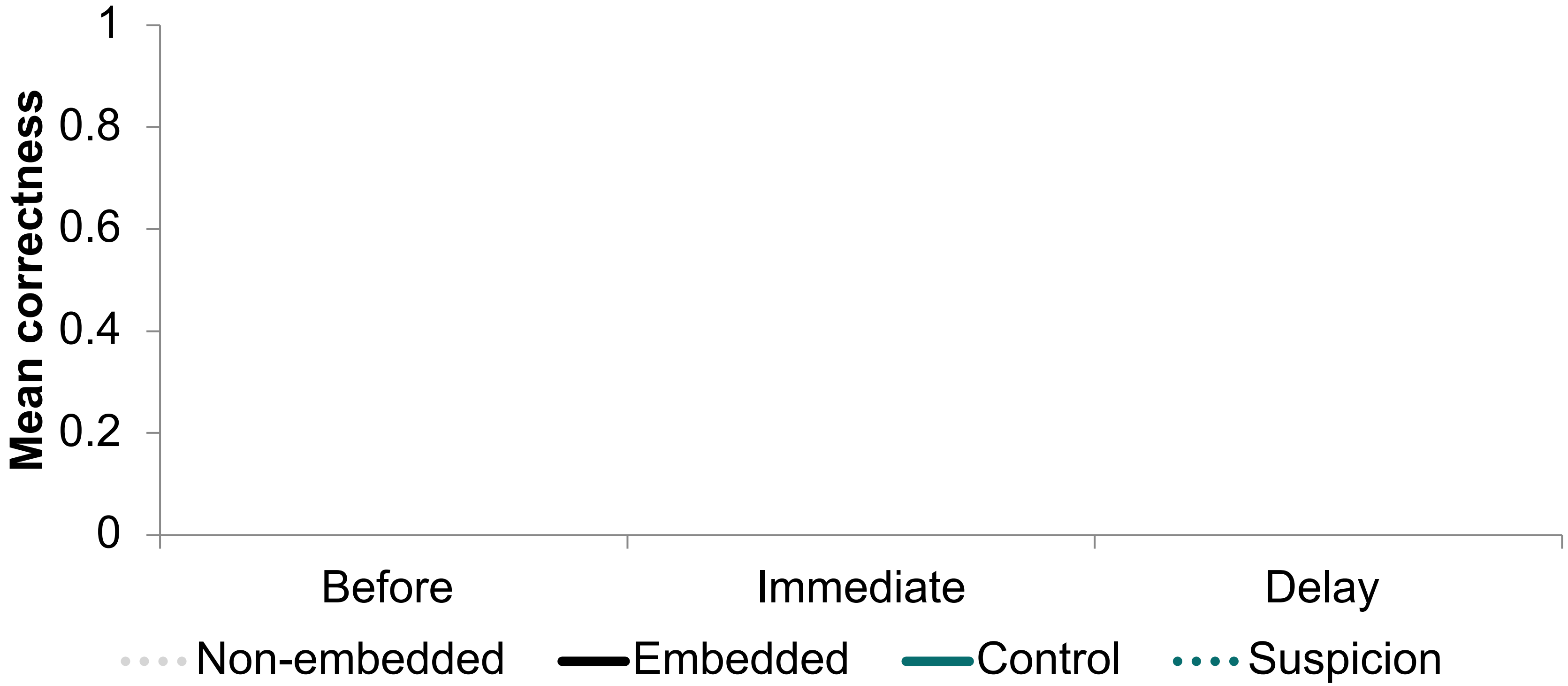
- 56 participants, 4 conditions
  - Control: no intervention
  - Suspicion: email from a friend
  - Non-embedded: in email
  - Embedded: intervention after clicking on link

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).

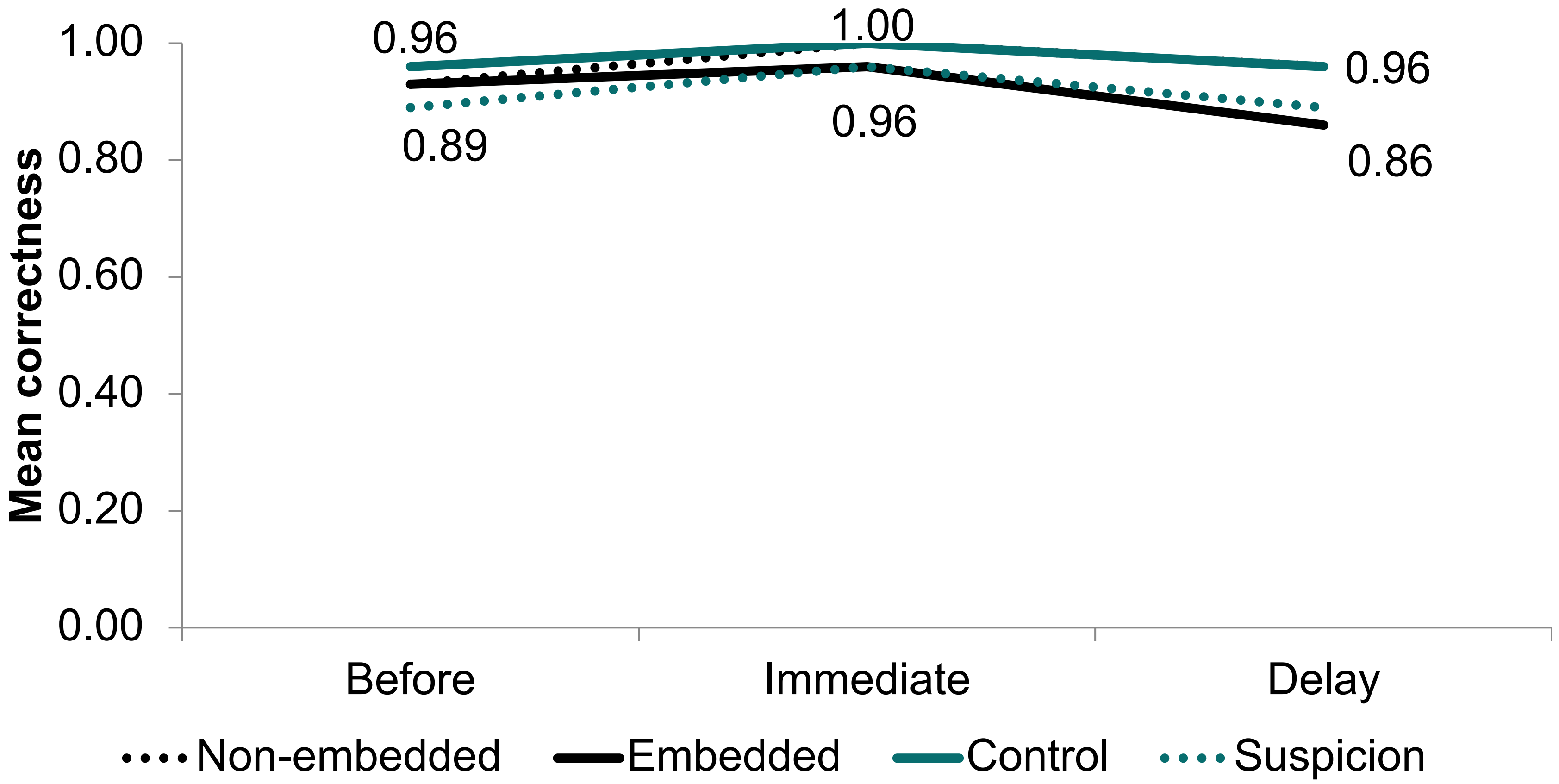
Some of Bobby’s messages

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

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

- Emailed all CMU students, faculty and staff to recruit participants to opt-in

- 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

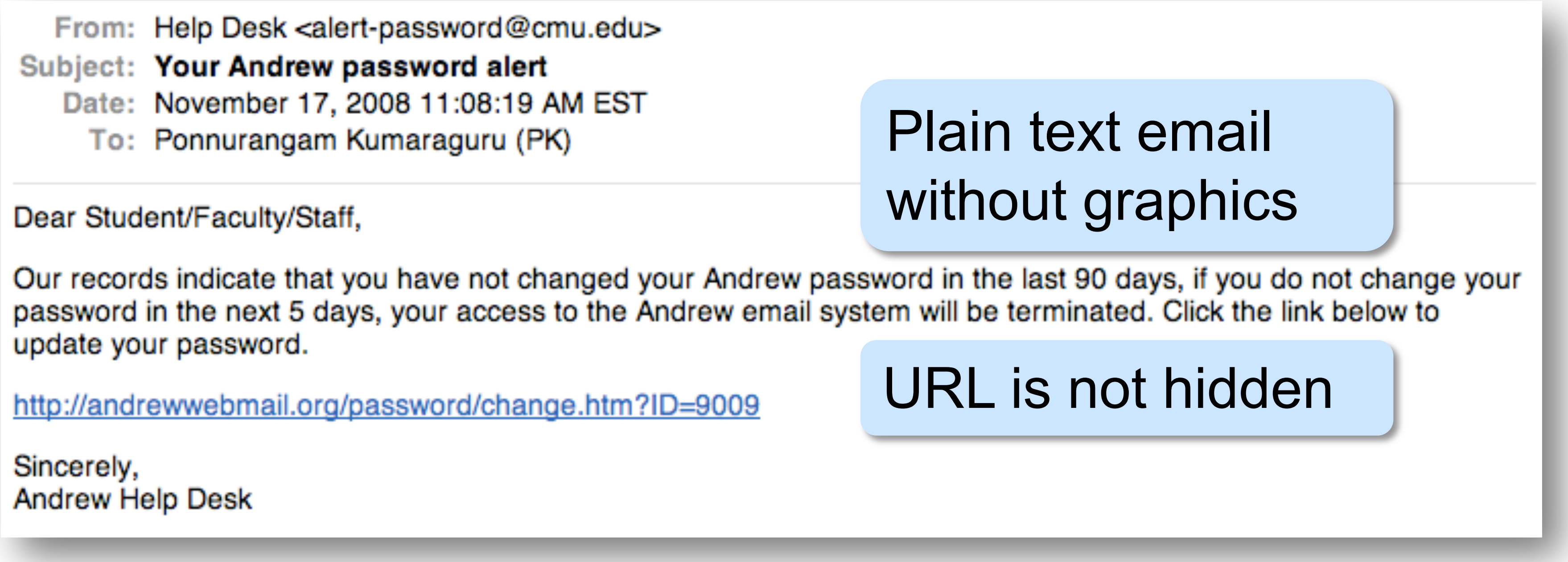
Implementation

- 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

<table>
<tr><th>Day of the study</th><th>Control</th><th>One training message</th><th>Two training messages</th></tr>
<tr><td>Day 0</td><td>Test and real</td><td>Train and real</td><td>Train and real</td></tr>
<tr><td>Day 2</td><td colspan="3">Test</td></tr>
<tr><td>Day 7</td><td colspan="3">Test and real</td></tr>
<tr><td>Day 14</td><td>Test</td><td>Test</td><td>Train</td></tr>
<tr><td>Day 16</td><td colspan="3">Test</td></tr>
<tr><td>Day 21</td><td colspan="3">Test</td></tr>
<tr><td>Day 28</td><td colspan="3">Test and real</td></tr>
<tr><td>Day 35</td><td colspan="3">Post-study survey</td></tr>
</table>

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)

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.

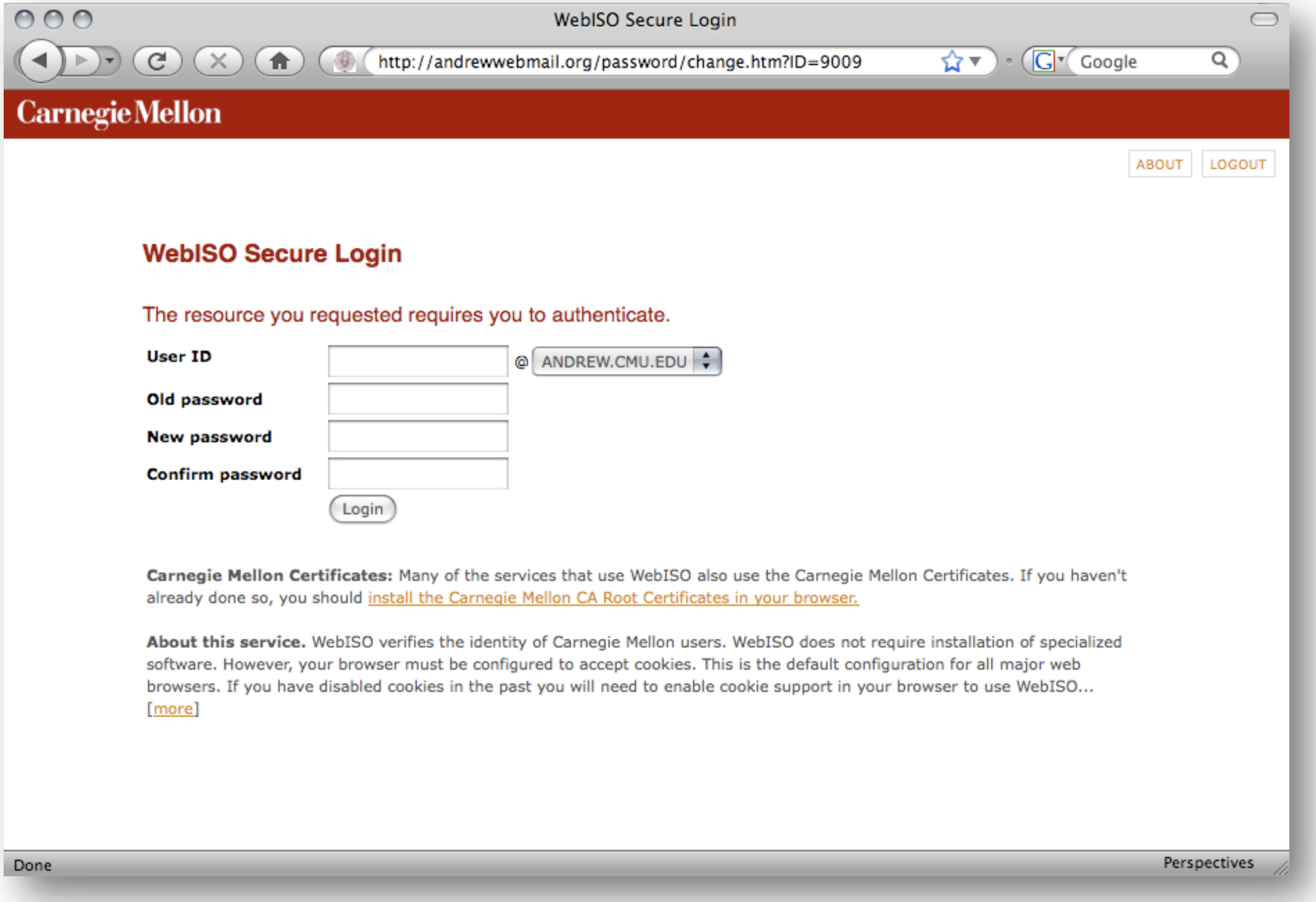
http://andrewwebmail.org/password/change.htm?ID=9009

Sincerely,
Andrew Help Desk

Plain text email without graphics

URL is not hidden

Simulated phishing website



WebISO Secure Login

The resource you requested requires you to authenticate.

User ID ____ @ ANDREW.CMU.EDU

Old password ____

New password ____

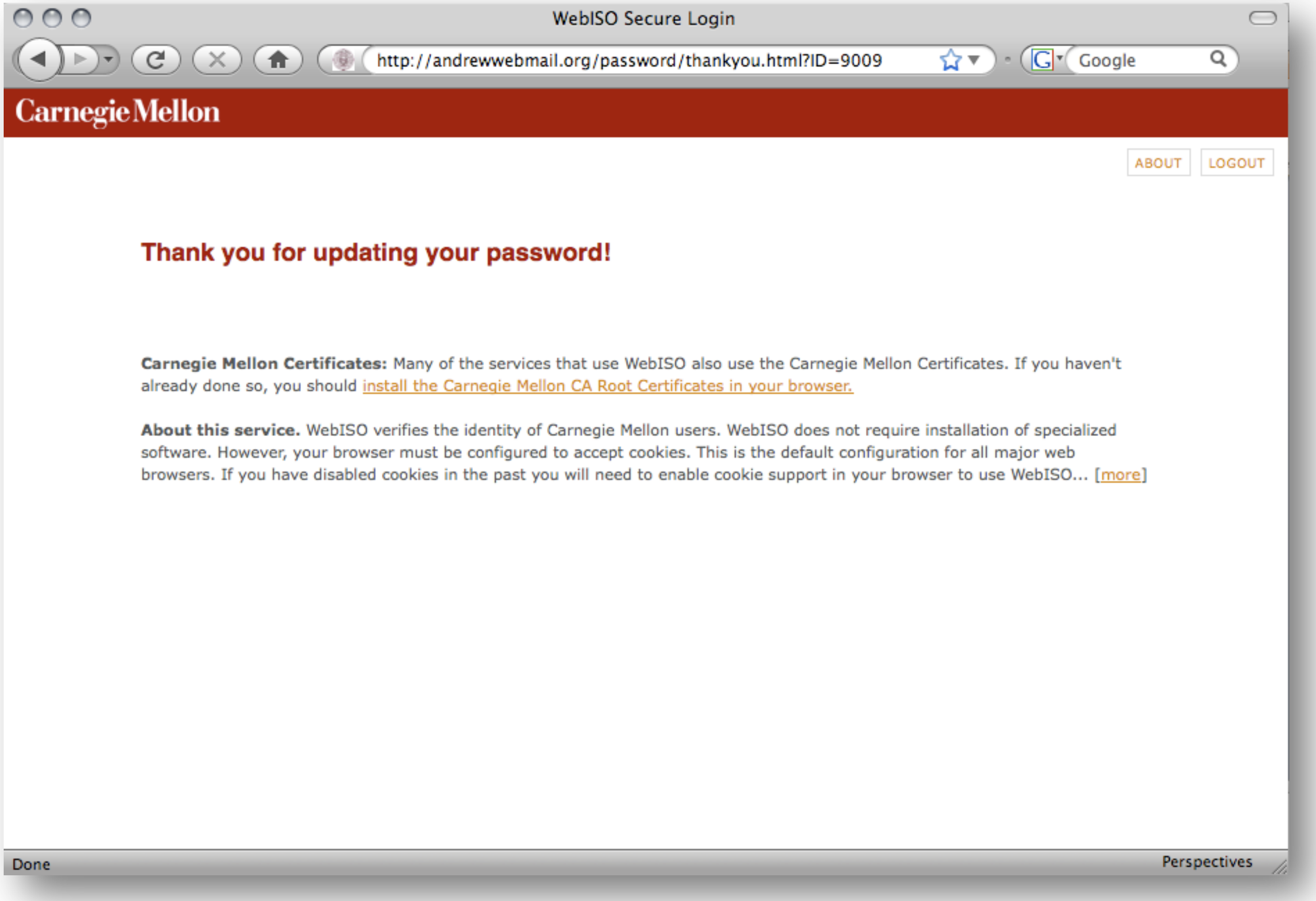
Confirm password ____

Login

Carnegie Mellon Certificates: Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, you should install the Carnegie Mellon CA Root Certificates in your browser.

About this service. WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [more]

Simulated phishing website

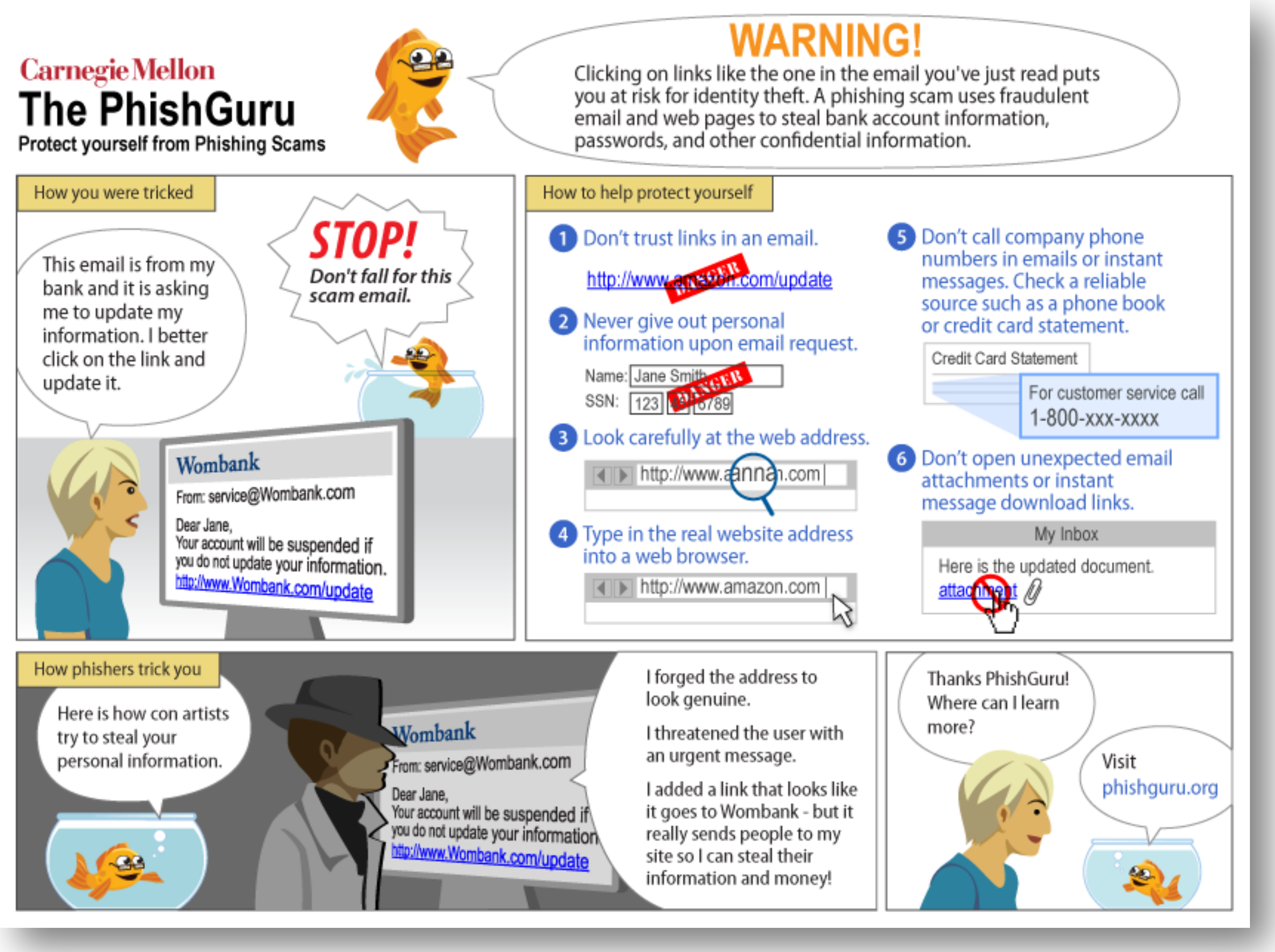


Thank you for updating your password!

Carnegie Mellon Certificates: Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, you should install the Carnegie Mellon CA Root Certificates in your browser.

About this service. WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [more]

PhishGuru intervention


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
SSN: 123 45 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.
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

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 (only half of people who clicked on day 0 clicked on day 28)

- 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 (students mostly likely to fall for phishing)

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!”

From research to reality

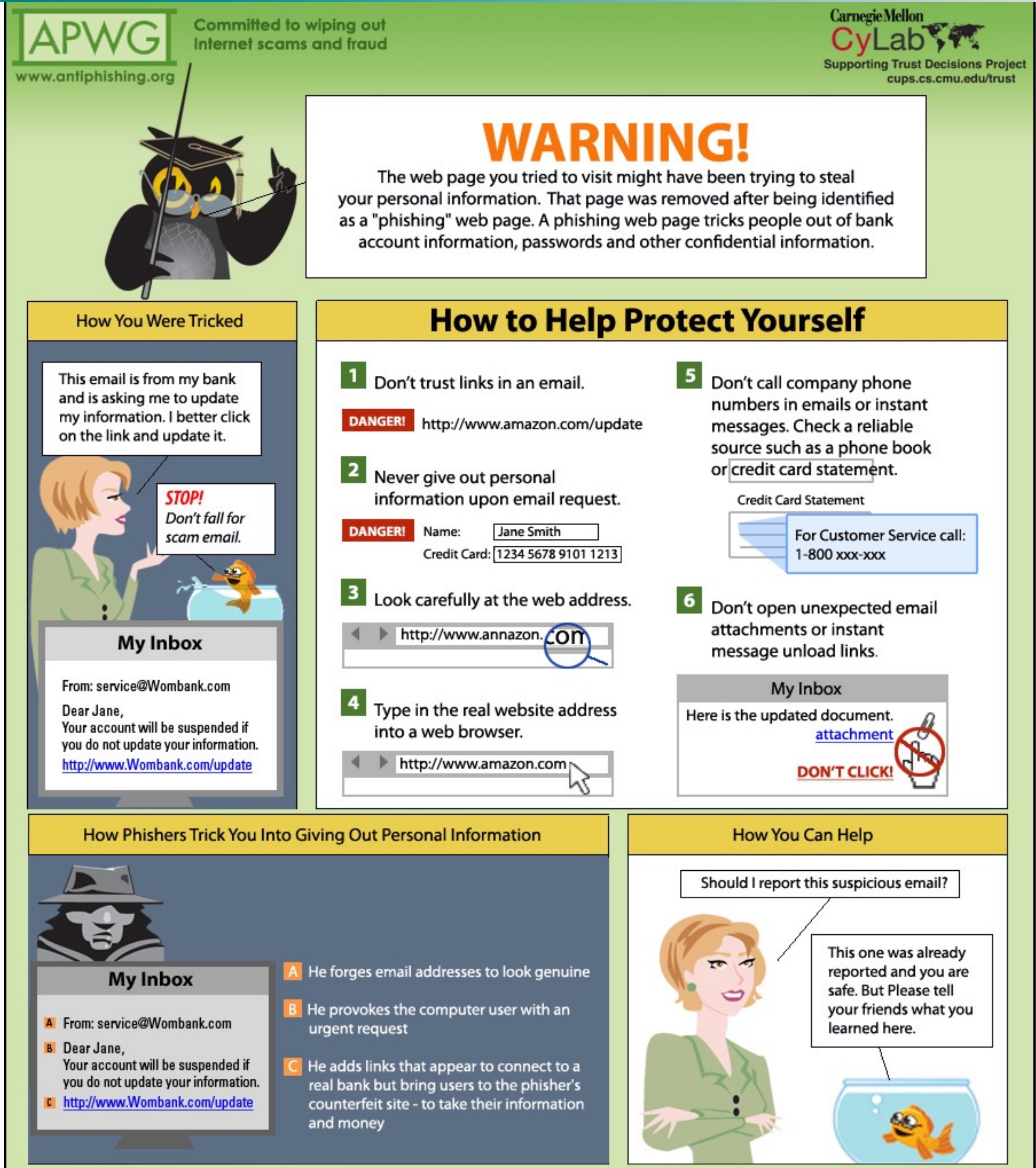
- Iterated on PhishGuru designs
- PhishGuru user studies
  - Laboratory
  - Real-world
- Anti-Phishing Working Group landing page
- PhishGuru commercialized by Wombat Security Technologies, Inc., acquired by Proofpoint in 2018

APWG landing page

- Train people when they fall for actual phishing emails
- Redirect people to “landing page”

http://education.apwg.org/

P. Kumaraguru, L. Cranor, and L. Mather. Anti-Phishing Landing Page: Turning a 404 into a Teachable Moment for End Users. CEAS 2009.



APWG
www.antiphishing.org
Committed to wiping out Internet scams and fraud

Carnegie Mellon CyLab
Supporting Trust Decisions Project
cups.cs.cmu.edu/trust

WARNING!
The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

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

STOP! Don't fall for scam email.

My Inbox
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.
DANGER! http://www.amazon.com/update

2 Never give out personal information upon email request.
DANGER! Name: Jane Smith
Credit Card: 1234 5678 9101 1213

3 Look carefully at the web address.
http://www.annazon.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-xxx

6 Don't open unexpected email attachments or instant message unload links.
My Inbox
Here is the updated document.
attachment
DON'T CLICK!

How Phishers Trick You Into Giving Out Personal Information

My Inbox
A From: service@Wombank.com
B Dear Jane,
Your account will be suspended if you do not update your information.
C http://www.Wombank.com/update

A He forges email addresses to look genuine
B He provokes the computer user with an urgent request
C He adds links that appear to connect to a real bank but bring users to the phisher's counterfeit site - to take their information and money

How You Can Help

Should I report this suspicious email?

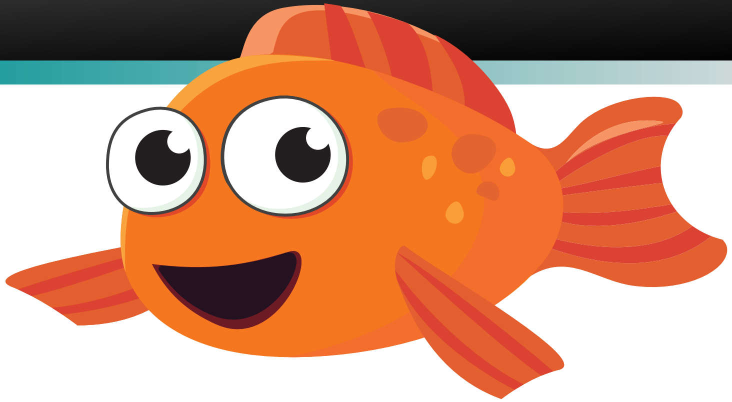
This one was already reported and you are safe. But Please tell your friends what you learned here.

How do we get people trained?

- Problem
  - 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
  - Existing (2010) materials good, but could be better

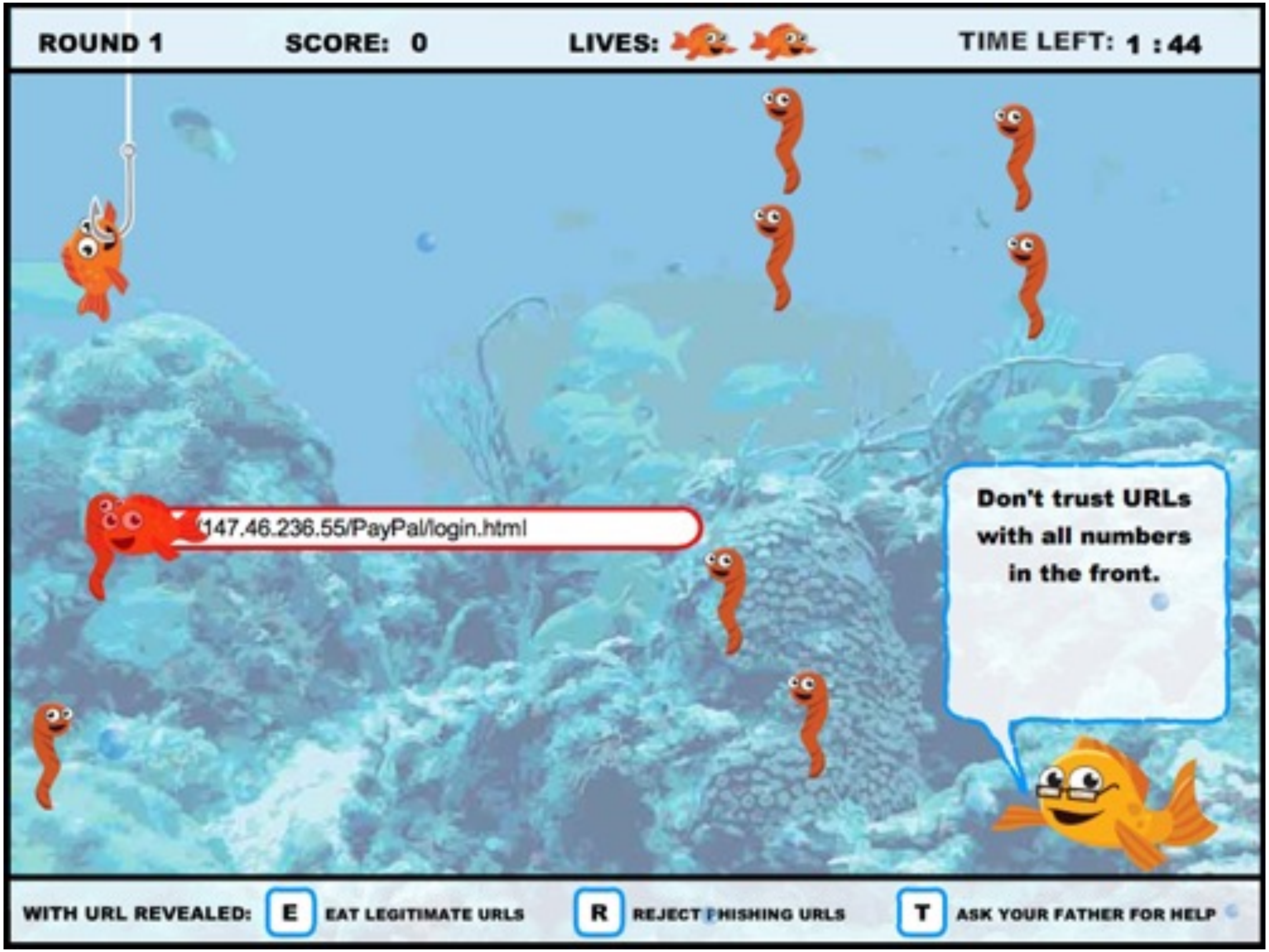
- Solution
  - Use learning science principles
  - Find a “teachable moment”: PhishGuru
  - Make training fun: Anti-Phishing Phil

Anti-Phishing Phil



- Online game
- Teaches people how to protect themselves from phishing attacks
  - identify phishing URLs
  - use web browser cues
  - find legitimate sites with search engines

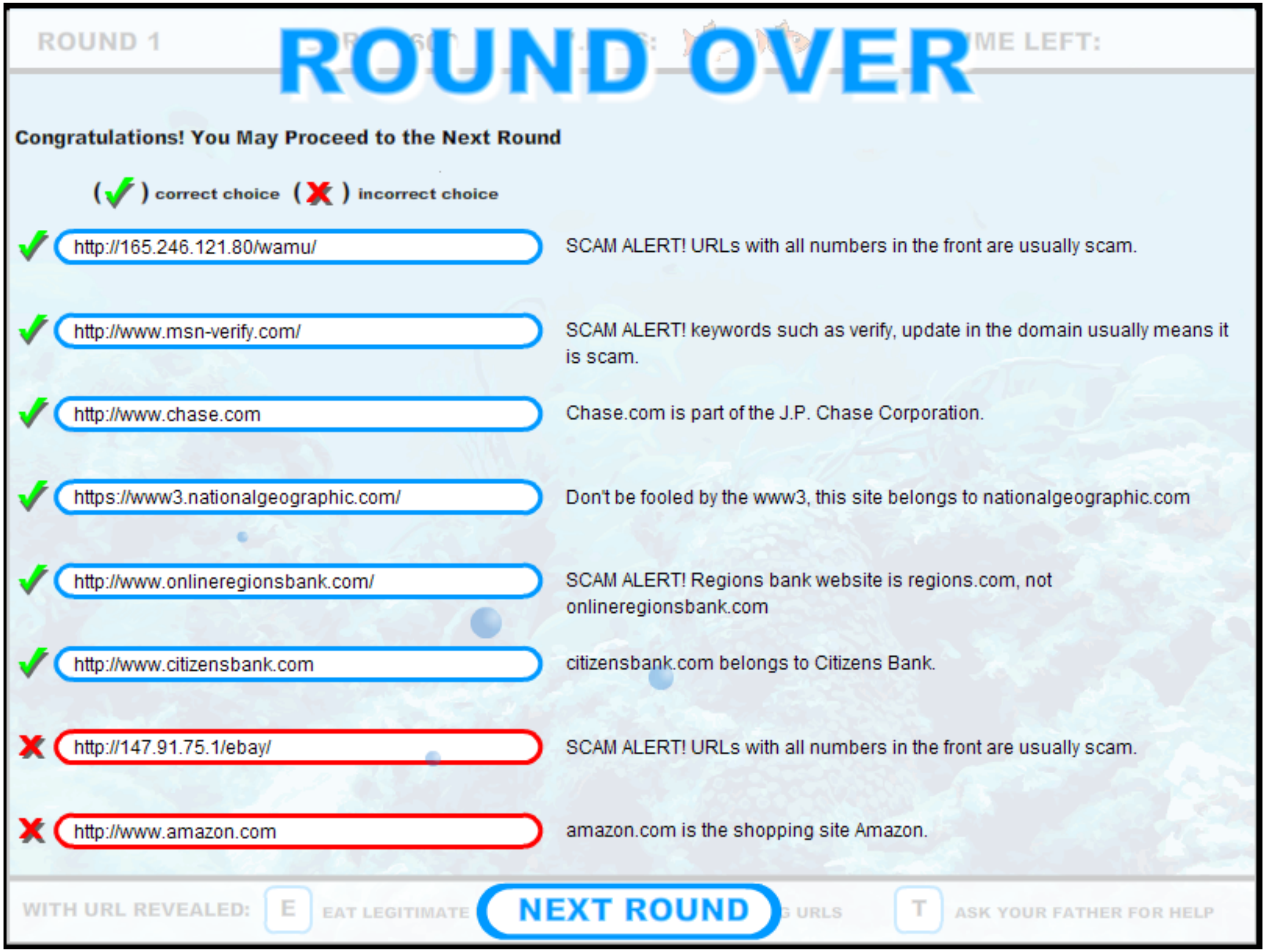
S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. SOUPS 2007.



ROUND 1 SCORE: 0 LIVES: TIME LEFT: 1 :44

(147.46.236.55/PayPal/login.html

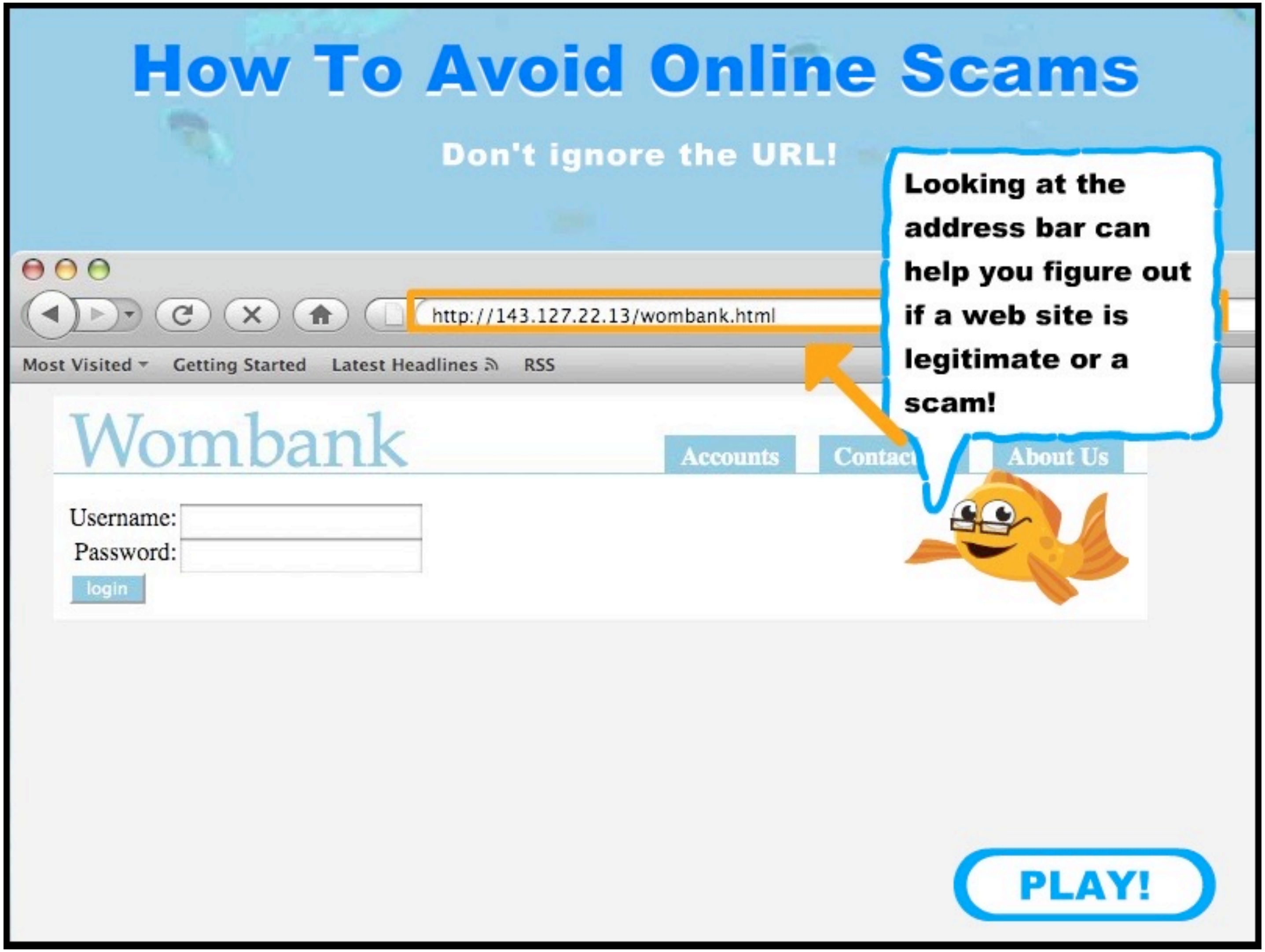
Don't trust URLs with all numbers in the front.



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.



How To Avoid Online Scams

Don't ignore the URL!

Looking at the address bar can help you figure out if a web site is legitimate or a scam!

http://143.127.22.13/wombank.html

Wombank

Username:

Password:

User Study 1

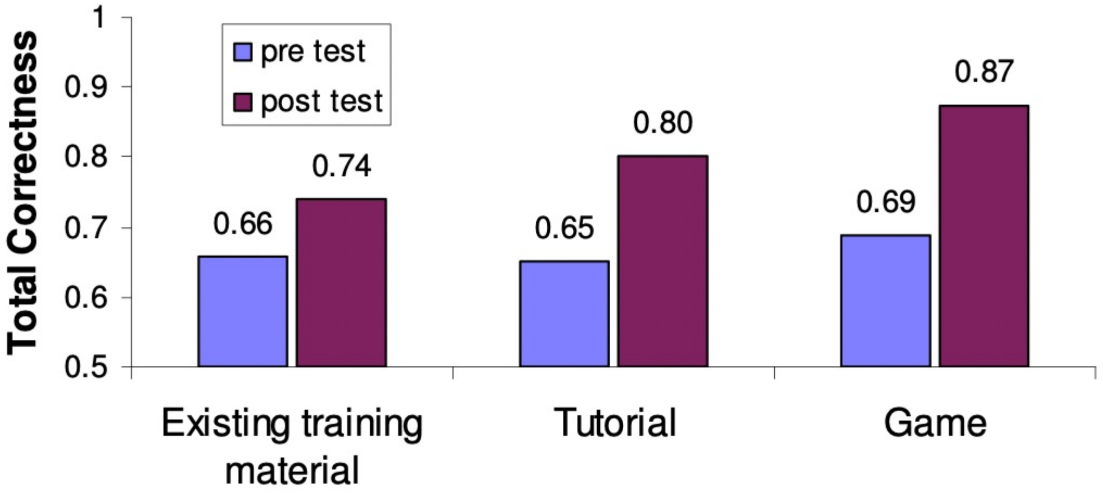
- Test participants’ ability to identify phishing web sites before/after training
  - 10 URLs before training, 10 after, randomized
  - Up to 15 minutes of training

- Three conditions:
  - Web-based phishing education
  - Tutorial
  - Game

- 42 participants (14 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 game was significantly better accuracy than existing



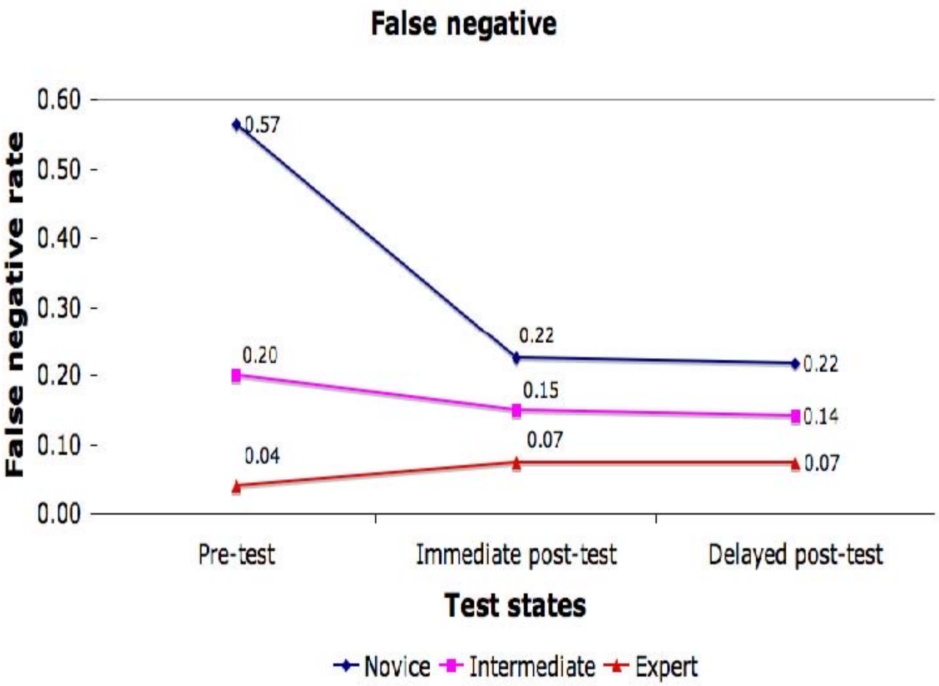
User Study 2

- Test participants’ ability to identify phishing web sites before/after training
  - 6 URLs each: before game, after game, 1 week later (randomized)

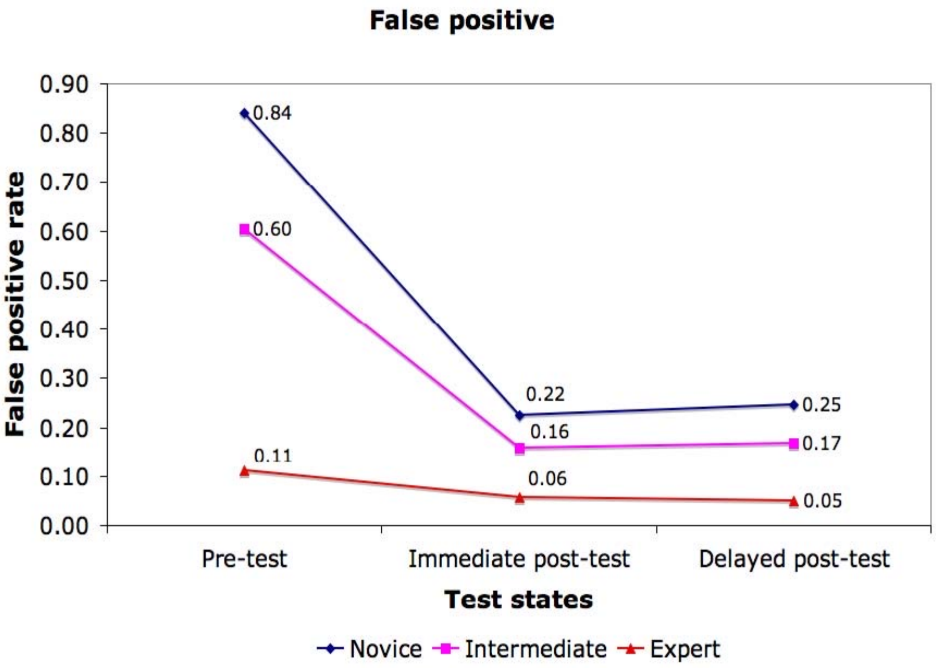
- 2,021 participants completed first phase, 674 completed 1 week later
  - Screened out security experts
  - Younger, college students

Anti-Phishing Phil in the Wild

False negatives

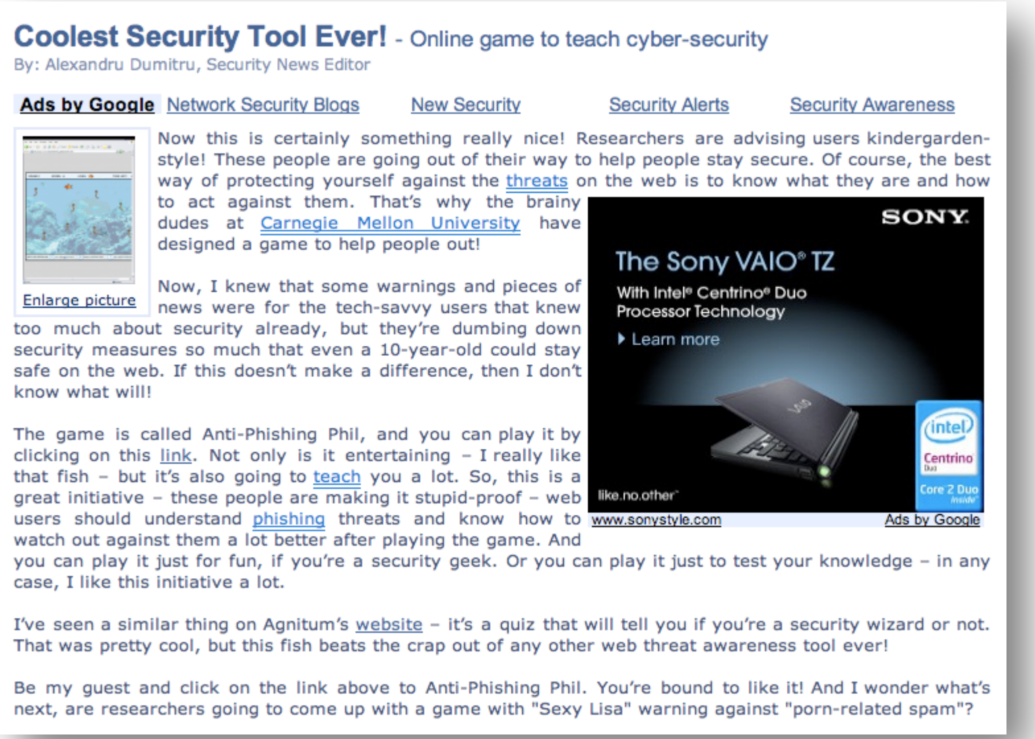


False positives



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 f compliance and Internet t
- “I plan to direct my mothe



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"?

Why is Phil so popular?

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

Security user education is possible

- Conventional wisdom: end-user security training does not work
- Anti-phishing 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

User education in security/privacy

- What areas would most benefit from user education? How might you design effective educational tools for that domain?

Phishing Prevention

ails. I will not open suspicious emails.
ails. I will not open suspicious emails.
ails. I will not open suspicious emails.
ails. I will not open suspicious emails.
ails. I will not open suspicio
Brown