24 – User education and phishing

Lujo Bauer, Nicolas Christin, and Abby Marsh

April 11, 2016
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
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
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
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
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
Spear-phishing

• Targets specific groups of individuals
  – Guesses email types/senders for that group
• Increasingly target employees instead of customers
• 91% of cyberattacks begin with a spear-phishing attack (Trend Micro, 2012)
• ~1 in 2 large businesses targeted

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

• Recover from attacks quickly
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.”

• “Security user education is a myth.”

• “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.”
How Not to Get Hooked by a ‘Phishing’ Scam

Quick Facts

Phishing is a scam where Internet fraudsters send you personal and financial information from unsolicited emails:

- Don't reply to email or pop-up messages that look like they are from your bank or other online account.
- Don't click on links in these emails.
- Use anti-virus and anti-spyware software, as they may contain malicious software.
- Don't email personal or financial information.
- Review credit card and bank account statements for unauthorized charges.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
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)*, 10(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 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!
<table>
<thead>
<tr>
<th>From</th>
<th>Date</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiona Jones</td>
<td>Mar 12, 2007</td>
<td>Will pick you up in 60 minutes</td>
</tr>
<tr>
<td>Zang Li</td>
<td>Mar 12, 2007</td>
<td>Conference room #2 - reservation</td>
</tr>
<tr>
<td>IKEA</td>
<td>Mar 12, 2007</td>
<td>Your IKEA order confirmation</td>
</tr>
<tr>
<td>eBay</td>
<td>Mar 12, 2007</td>
<td>Reactivate your eBay account</td>
</tr>
<tr>
<td>Mary Allen</td>
<td>Mar 12, 2007</td>
<td>How about lunch together tomorrow?</td>
</tr>
<tr>
<td>Eleanor Fitzpatrick</td>
<td>Mar 12, 2007</td>
<td>sexy baby and bad erection?</td>
</tr>
<tr>
<td>Joseph Dicosta</td>
<td>Mar 12, 2007</td>
<td>tomorrow's meeting rescheduled</td>
</tr>
<tr>
<td>Monika Berdford</td>
<td>Mar 12, 2007</td>
<td>View my photos on Yahoo! Photos</td>
</tr>
<tr>
<td>Joseph Dicosta</td>
<td>Mar 12, 2007</td>
<td>document dropped - your office - please fax</td>
</tr>
<tr>
<td>Barclays Bank</td>
<td>Mar 12, 2007</td>
<td>Update your account information</td>
</tr>
<tr>
<td>Jean Williams</td>
<td>Mar 12, 2007</td>
<td>Sushi making party</td>
</tr>
<tr>
<td>Ni Cheng</td>
<td>Mar 12, 2007</td>
<td>[cognito] Dinner menu selection - Annual day</td>
</tr>
<tr>
<td>CitiBank</td>
<td>Mar 12, 2007</td>
<td>Citibank Urgent E-mail Verification</td>
</tr>
<tr>
<td>Zang Li</td>
<td>Mar 12, 2007</td>
<td>Business cards</td>
</tr>
<tr>
<td>Jesse</td>
<td>Mar 12, 2007</td>
<td>A warm Hello from Jesse</td>
</tr>
</tbody>
</table>

Subject: Revision to Your Amazon.com Information
Subject: Revision to Your Amazon.com Information

Please login and enter your information

Please follow this link to update your personal information:


(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 until you have the time to contact us by phone.

We appreciate 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.
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.9999.com/update

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123-45-6789

3. Look carefully at the web address.
   http://www.annn.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.

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
Applies learning-by-doing and immediate feedback principles.
Applies story-based agent principle
How to help protect yourself

1. Don’t trust links in an email.
   http://www.amazon.com/update

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123-456-789

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

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.

Tips:
- For customer service call 1-800-xxx-xxxx

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

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 suspened if you do not update your information.
http://www.Wombank.com/update

Site so I can steal their information and money!

Applies contiguity principle
Presents procedural knowledge
Applies personalization principle
Presents conceptual knowledge
Carnegie Mellon - The PhishGuru

The PhishGuru

Protect yourself from Phishing Scams

How you were tricked

STOP!

Don't fall for this scam email.

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.com

Dear Jane,
Your account will be suspended if you do not update your information.

http://www.Wombank.com/update

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.phishguru.com/update

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123-45-6789

3. Look carefully at the URL of any link in an email.

4. Type in the valid URL into a web browser instead of clicking on a link in an email.

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.

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.

Visit phishguru.org

Thanks PhishGuru! Where can I learn more?
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 kinds of phishing scams.

2. What does a phishing scam look like?

Subject: Revision to Your Amazon.com Information
From: "Amazon" <service@amazon.com>
Date: Tue, April 11, 2006 4:04 pm
To: bsmith@cognix.com
Priority: Normal
Options: View Full Header! View Printable Version

PHISHING SCAM EXAMPLE

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 don't have enough information about our clients, we require this verification. Please login and reenter your personal information.

Please follow this link to update your personal information:

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

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

http://www.amazonaccount.net/exec/obidos/flex-sign-in.htm?104-2497720-3229513

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.

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.
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. Scammer plans attack...
   - I can make a professional & legitimate looking email impersonating a well-known company.

2. User receives scam...
   - Let's check what the new email is about.

3. Scammer forges sender's address to look genuine.
   - From: service@amazon.com

4. User threatens users account status with urgent message.
   - Your account will be suspended if you don't update your info.

5. Scammer threatens users account status with urgent message.
   - http://amazon.com/update

6. User includes a disguised link within the email.
   - http://www.amazon.com/update

7. Scammer includes a disguised link within the email.
   - To: Amazon Member

8. User will send this email to many users.

9. User asks for my ID & password, and link looks suspicious. I never click on link within emails.
   - From: service@amazon.com
   - Subject: Revision to Your Account
   - http://amazon.com/link
   - http://amazon-link.net/account

10. Scammer will never give up my personal information upon email request.
   - Username:
   - Password:
   - SSN:
   - Credit Card:

11. User will never allow scammers to steal my precious identity!
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.

The Phisher

I can create my own emails that look just like the messages that big companies send out.

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@myemail.com
amazon.com

Your account will be suspended if you do not update your account information.

http://www.amazon.com/update

This email looks very professional! I’ll send it to thousands of people.

The Victim

I better click on this link and update my information.

YOU’VE GOT MAIL!

STOP! Follow these steps when reading your email:

1. Never click on links within emails.
   http://www.amazon.com/update

2. Find and call a real customer service center.

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

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

5. Always be wary of suspicious websites.

Thanks PhishGuru! I will never let phishers steal my identity.
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.

**The Phisher**

I can create my own emails that look just like the messages that big companies send out.

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

This email looks very professional! I'll send it to thousands of people.

**The Victim**

STOP! Follow these steps when reading your email.

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.

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

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123-45-6789

3. Look carefully at the web address.
   http://www.african.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.
   attach it

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

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

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.2snn.com/update

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123 456 789

3. Look carefully at the web address.
   http://www.2nn.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.

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

How phishers trick you

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!

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.

For customer service call 1-800-xxx-xxxx

My Inbox
Here is the updated document.

Thanks. Where can I learn more?

Visit phishguru.org
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?

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

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

Mean correctness

Before  Immediate  Delay

0.04
Results - Phishing account emails

![Graph showing mean correctness for different conditions: Non-embedded, Embedded, Control, and Suspicion. The graph includes data points for Before, Immediate, and Delay stages. Mean correctness values for each condition are shown at different time points.]
Results - Phishing account emails

Mean correctness

- Before
  - Non-embedded: 0.04
  - Embedded: 0.18
  - Control: 0.07
  - Suspicion: 0.68

- Immediate
  - Non-embedded: 0.04
  - Embedded: 0.68
  - Control: 0.07
  - Suspicion: 0.64

- Delay
  - Non-embedded: 0.04
  - Embedded: 0.07
  - Control: 0.07
  - Suspicion: 0.64
Results - Phishing account emails

![Graph showing mean correctness for different conditions: Non-embedded, Embedded, Control, and Suspicion. The graph demonstrates an increase in mean correctness from Before to Immediate and a decrease from Immediate to Delay.](image-url)
Results - Phishing account emails

[Graph showing mean correctness for non-embedded, embedded, control, and suspicion categories across Before, Immediate, and Delay phases.]

- Mean correctness for non-embedded before immediate delay: 0.04
- Mean correctness for embedded before immediate delay: 0.04
- Mean correctness for control before immediate delay: 0.04
- Mean correctness for suspicion before immediate delay: 0.04

- Mean correctness for non-embedded immediate delay: 0.18
- Mean correctness for embedded immediate delay: 0.68
- Mean correctness for control immediate delay: 0.64
- Mean correctness for suspicion immediate delay: 0.07
Results – Legitimate link emails

- Before Immediate Delay
  - Mean correctness
    - Non-embedded
    - Embedded
    - Control
    - Suspicion

Graph showing mean correctness for different conditions: non-embedded, embedded, control, and suspicion categories.
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

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

<table>
<thead>
<tr>
<th>Day of the study</th>
<th>Control</th>
<th>One training message</th>
<th>Two training messages</th>
</tr>
</thead>
<tbody>
<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></td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>Day 7</td>
<td></td>
<td>Test and real</td>
<td></td>
</tr>
<tr>
<td>Day 14</td>
<td>Test</td>
<td>Test</td>
<td>Train</td>
</tr>
<tr>
<td>Day 16</td>
<td></td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>Day 21</td>
<td></td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>Day 28</td>
<td></td>
<td>Test and real</td>
<td></td>
</tr>
<tr>
<td>Day 35</td>
<td></td>
<td>Post-study survey</td>
<td></td>
</tr>
</tbody>
</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
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...
PhishGuru intervention

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams

STOP!
Don’t fall for this scam email.

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.

How phishers trick you
Here is how con artists try to steal your personal information.

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 to help protect yourself

1. Don’t trust links in an email.
   http://www.amazon.com/update

2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123-45-6789

3. Look carefully at the web address.
   http://www.amazon.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.

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

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

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>N</th>
<th>% who clicked on Day 0</th>
<th>% who clicked on Day 28</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>172</td>
<td>52.3</td>
<td>44.2</td>
</tr>
<tr>
<td>Trained</td>
<td>343</td>
<td>48.4</td>
<td>24.5</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>N</th>
<th>Day 0</th>
<th>Day 7</th>
<th>Day 28</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>90</td>
<td>50.0</td>
<td>41.1</td>
<td>38.9</td>
</tr>
<tr>
<td>One-train</td>
<td>89</td>
<td>39.3</td>
<td>42.7</td>
<td>32.3</td>
</tr>
<tr>
<td>Two-train</td>
<td>77</td>
<td>48.1</td>
<td>44.2</td>
<td>35.1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>N</th>
<th>Day 0 Clicked %</th>
<th>Day 7 Clicked %</th>
<th>Day 28 Clicked %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>90</td>
<td>50.0</td>
<td>41.1</td>
<td>38.9</td>
</tr>
<tr>
<td>One-train</td>
<td>89</td>
<td>39.3</td>
<td>42.7</td>
<td>32.3</td>
</tr>
<tr>
<td>Two-train</td>
<td>77</td>
<td>48.1</td>
<td>44.2</td>
<td>35.1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Age group</th>
<th>Day 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-25</td>
<td>62%</td>
</tr>
<tr>
<td>26-35</td>
<td>48%</td>
</tr>
<tr>
<td>36-45</td>
<td>33%</td>
</tr>
<tr>
<td>45 and older</td>
<td>43%</td>
</tr>
</tbody>
</table>
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!”
Train people when they fall for actual phishing emails
- Redirect people to "landing page"
- CMU collecting and analyzing log files
- http://education.apwg.org/
Anti-phishing Phil
Anti-Phishing Phil

- Online game
- [http://wombatsecurity.com/antiphishingphil](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

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.onlinerregionsbank.com/  SCAM ALERT! Regions bank website is regions.com, not onlinerregionsbank.com


✗ 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!
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.
Is this the real eBay website?

REAL  FAKE  1/6

Sell: Register or Sign In

Now 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
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 negative results graph]

- **False negative rate**
  - **Test states**: Pre-test, Immediate post-test, Delayed post-test
  - **Categories**: Novice, Intermediate, Expert

- **Novice**
  - Pre-test: 0.57, Immediate post-test: 0.22, Delayed post-test: 0.22

- **Intermediate**
  - Pre-test: 0.20, Immediate post-test: 0.15, Delayed post-test: 0.14

- **Expert**
  - Pre-test: 0.04, Immediate post-test: 0.07, Delayed post-test: 0.07
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.”
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
- 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