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

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
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 the 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,
Safe harbor 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&signln&sid=verify&co_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll&signln&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,
Safe harbor 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 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
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
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.”

- “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

Phishing is a scam where Internet fraudsters send you a fake Web site that requests personal and financial information from users who visit it. These sites can look like they go one place, but actually link to a different page.

Some scammers send an email that appears to be from a PayPal employee. In the email, the fraudster asks you to call a phone number on the email to discuss a pending transaction. The number on the email may look legitimate, but it is not.

Use anti-virus and anti-spyware software, and keep it up to date. Install the latest security updates for your computer.

Don’t email personal or financial information.

Review credit card and bank account statements regularly.

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 they had more false positives
- People can learn from web-based training materials, if only we could get them to read them!

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
<table>
<thead>
<tr>
<th>From</th>
<th>Date</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jesse Smith</td>
<td>Apr 11, 2006</td>
<td>Will pick you up in 90 minutes</td>
</tr>
<tr>
<td>Joseph Dicosta</td>
<td>Apr 11, 2006</td>
<td>tomorrow's meeting rescheduled</td>
</tr>
<tr>
<td>Brandy Anderson</td>
<td>Apr 11, 2006</td>
<td>Re: tomorrow's meeting rescheduled ?</td>
</tr>
<tr>
<td>Ni Cheng</td>
<td>Apr 11, 2006</td>
<td>Paragraph to check</td>
</tr>
<tr>
<td><a href="mailto:julie@cognix.com">julie@cognix.com</a></td>
<td>Apr 11, 2006</td>
<td>great article</td>
</tr>
<tr>
<td>Ni Cheng</td>
<td>Apr 11, 2006</td>
<td>[cognix-marketing] REMINDER: Power Shut-Down This Satu...</td>
</tr>
<tr>
<td>Brandy Anderson</td>
<td>Apr 11, 2006</td>
<td>Welcome Jennifer to email</td>
</tr>
<tr>
<td>hamza sani</td>
<td>Apr 11, 2006</td>
<td>REPLY QUICKLY PLEASE</td>
</tr>
<tr>
<td>Jean Williams</td>
<td>Apr 11, 2006</td>
<td>cool pic</td>
</tr>
<tr>
<td>Security Advisor</td>
<td>Apr 11, 2006</td>
<td>Update your account information</td>
</tr>
<tr>
<td>Ni Cheng</td>
<td>Apr 11, 2006</td>
<td>[cognix-marketing] Dinner menu selection - Annual ...</td>
</tr>
<tr>
<td><a href="mailto:service@paypal.com">service@paypal.com</a></td>
<td>Apr 11, 2006</td>
<td>Reactivate Your PayPal Account!</td>
</tr>
<tr>
<td>Jean Williams</td>
<td>Apr 11, 2006</td>
<td>Re: Funny joke (fwd)</td>
</tr>
<tr>
<td>Fiona Jones</td>
<td>Apr 11, 2006</td>
<td>Don't forget mom's birthday!</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:

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.

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.
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

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.

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.amazon.com

4. Type in the real website address into a web browser.
http://www.wombank.com/update

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.

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
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

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

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

<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
Simulated phishing website

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

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

### 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.

### 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.example.com/update](http://www.example.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.example.com](http://www.example.com)

4. Type in the real website address into a web browser.
   
   ![http://www.amazon.com](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](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](My Inbox)
   
   Here is the updated document.
   
   ![attaching](attaching)

### 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.


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](http://www.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 Services</td>
<td>Congratulation - Plaid Ca$h</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
## 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
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></td>
<td></td>
<td>Clicked %</td>
<td>Clicked %</td>
<td>Clicked %</td>
</tr>
<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>
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
How to protect yourself
Don’t trust links in an email

http://www.amazon.com/update
Never give out personal information upon email request.

Name: Jane Smith
SSN: 123 45 6789
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/

Learn how to protect yourself from phishing attacks.

http://phishguru.org/
Backup slides
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 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: 123-45-6789

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.

For customer service call 1-800-xxx-xxxx

Applies contiguity principle
Presents proceduralural knowledge
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 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!

Applies personalization principle
Presents conceptual knowledge
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.

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: [removed]

3. Look closely at the email header to see if the address is correct.

4. Type in the URL into a web browser, instead of clicking on a link.

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.

Thanks PhishGuru! Where can I learn more?
Visit phishguru.org
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.

From: service@amazon.com
To: molly@mymail.com

amazon.com

Then I threatened the user with an urgent message.

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.

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.

   annamazon.com

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.amazon.com/update (BANGER)
2. Never give out personal information upon email request.
   Name: Jane Smith
   SSN: 123 1231789
3. Look carefully at the web address.
   http://www.banana.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.
   For customer service call 1-800-xxx-xxxx
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.

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
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?

Follow these steps to protect yourself:

1. Don't trust links in an email.
   [Danger: http://www.equation.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.amanz.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:
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