The APWG/CMU Phishing Education Landing Page Project

education.apwg.org/r

Committed to wiping out Internet scams and fraud
Education Opportunities Lost

Phishing sites identified

Phishing sites taken down

Consumers click on links

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the httpd.apache.org home page, and then look for links to the information you want.
- Click the Back button to try another link.
- Click Search to look for information on the Internet.

HTTP 404 - File not found
Internet Explorer
Let’s Leverage This Common Resource for Education

• Redirect pages used for warning customers by some companies for different kinds of security events
• Carnegie Mellon University Researcher demonstrated a landing page Oct. 2007
• Designed specifically for consumer education on phishing – and how to avoid it
• Let’s look at an early CMU prototype:
CMU Landing Page

Quick & focused lesson

Easily digestible

Easy on the eye

Makes the best of a ‘teachable moment’
Project Initialized

- Immediate response: practical idea
- Bank of America delegate: bank looking at the idea previously and excited to see it manifested by a major research institute
- APWG Internet Policy Committee (IPC) took it up and looked at ways to expand the instruction the page provided to be more comprehensive
Design by Committee

• APWG member feedback on initial designs provided lots and lots and lots of suggestions and ideas
• And more ideas - And comments
• And Expert Opinions. Lots and lots
• Initial design used all of them
• Let’s look at the initial APWG/CMU Prototype
Warning!
The webpage you tried to access might have been trying to steal your personal information.

Help Protect Yourself from Identity Theft

Don't trust 'urgent' demands for personal information such as passwords in email, in instant messages or in cell telephone text messages.

STOP. Think: Avoid being rushed into giving up secrets or personal information you will later regret giving away.

Don't trust links in email, in instant messages or in cell telephone text messages. They can lead to viruses and infect your computer, handheld device or cell telephone.

DANGER!
Click here to log in:
http://www.abcbankexample.com

Don't trust company telephone numbers in email, in instant messages, in cell telephone text messages or even in CallerID displays.

DANGER!
*For more information, please call customer service: 1-800-123-...

DANGER!
ABC Bank Your account will be suspended if you don't update your information

MANUALLY TYPE the URLs for websites you need to visit, or use bookmarks you have created.

www.abcbank.com

LOOK UP telephone numbers using an established source. Use a telephone directory, a paper account statement or the telephone numbers on the back of your ATM cards and credit cards.

For account inquiries call:
1-800-XXX-XXX
Here is how con artists known as "phishers" try to steal your personal information:

I create scam email that looks just like real email from companies you trust.

"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 bank, but really it sends people to my site so I can steal their personal information!"

What You Should Do When You Receive a Suspicious Email or Electronic Message

CONSUMERS: Do not open, reply to or click on any links in a suspicious email. DELETE it.

ENTERPRISE USERS: Learn and abide by company policies on handling suspicious emails. Don't have a company policy on suspicious email? Suggest that such a policy be created.
MUCH
Consolidating the Suggestions Ideas Comments, Insights & Opinions . . .

- All ideas gathered around three topical principals:
  - Develop and use a skeptical eye
  - Practice good navigational habits
  - Practice sound computer hygiene
Final design

- Cartoon format designed with horizontal text in rectangular boxes so that text can all be HTML
- Suggests something for would-be victims to do (tell their friends)
- Only one link for more info, short URL spelled out in text
- Explain what APWG is at top
- Define phishing on first use
- Reduced number of instructions (omitted virus checking and patching)
Time to Deploy

APWG’s Swashbuckling Internet Safety Engineers Met to develop working specification for landing page
Working Specification

• Had to be nearly as nearly work-free as possible for ISPs to co-operate
• Had to work for all devices – handhelds as well as laptops and PCs
  - In many countries, online banking is mediated on a cell phone or handheld
• Had to work for all languages automatically
Working System

• PHP scheme
• ISP redirects users who’ve clicked on links to decommissioned websites to http://education.apwg.org/r
• PHP system reads Web access logs
  – Parses browser language setting
  – Parses browser type – indicating device
• PHP reaches into database and serves up version for user requirements
The Illustrated Page

**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.

**How to Help Protect Yourself**

1. Don't trust links in an email.
   
   **DANGER:** [http://www.amazon.com/update](http://www.amazon.com/update)

2. Never give out personal information upon email request.

   **DANGER:** Name: Jane Smith
   Credit Card: 1234 5578 9101 1213

3. Look carefully at the web address.

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.png)
   For Customer Service call: 1-800 xxx xxx

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

   ![Email Attachment](email_attachment.png)
Warning!

The web page you tried to visit might have been trying to steal your personal information. The link you clicked to get here was probably created by con artists.

That page was removed after being identified as a "phishing" web page. A phishing web page is created to trick people out of bank account information, passwords and other confidential information.

Help Protect Yourself from Identity Theft

- Don't trust 'urgent' demands for personal information such as passwords in email or in instant messages.
  > STOP. Think. Avoid being rushed into giving up secrets or personal information you will later regret giving away.
- Don't trust links in email or in instant messages. They can lead to viruses and infect your computer.
  > MANUALLY TYPE the URLs for websites you need to visit, or use bookmarks you have created.
- Don't trust company telephone numbers in email or in instant messages.
  > LOOK UP telephone numbers using an established source. Use a telephone directory, a paper account statement or the telephone numbers on the back of your ATM cards and credit cards.
- Don't trust unexpected email attachments or instant message download links.
  > SCAN all attachments for viruses even in expected emails from friends and colleagues.

Legal Disclaimer

- PLEASE NOTE: The APWG, CMU's Supporting Trust Decisions Project and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phished or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid phishing and malware attacks. You can find more information at the APWG website: http://www.apwg.org.

Committed to wiping out Internet scams and fraud
Implementation and results

• It works
• In English, French, Spanish, Hungarian, Ukranian and more to come
• Being translated into 15 languages
• 1 Oct, 2008 – 1 March, 2009
  – 56,699 “teachable moments”
  – Average number of days: 34.9 days
  – 87.8% hits are from the US
Development Program

• Keep developing translations for every language in which phishing becomes a problem
• Promote usage among ISPs
• Analyze data for trends and insights
Questions ?
Thankest

• Peter Cassidy
• pcassidy@antiphishing.org
• +1 617 669 1123