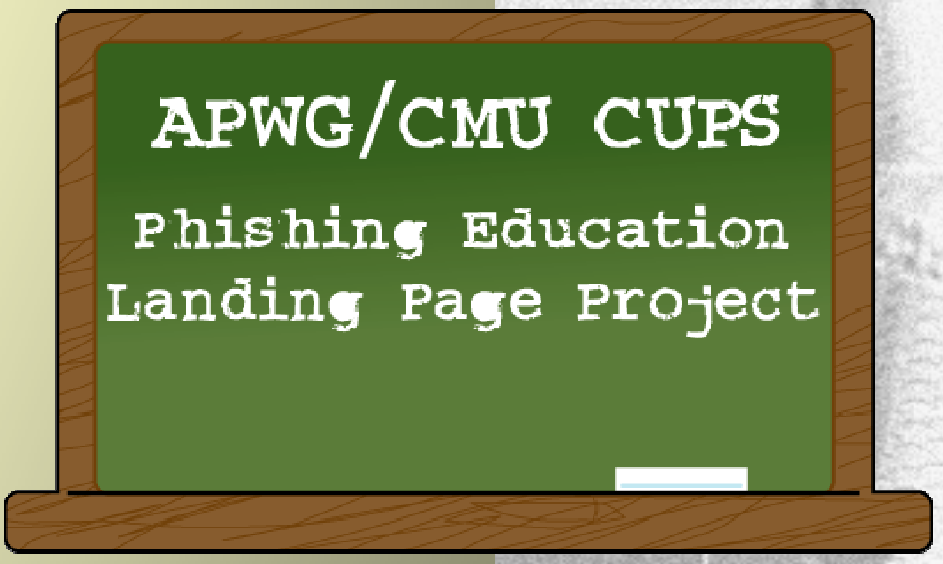
Optimizing Counter-eCrime Consumer Education Through Just-in-Time Delivery of Computer Safety Instruction

An APWG Public Education Initiative Program



April 2009

Correspondent Authors and Application Architects' Contact Data:
Lorrie Cranor, Carnegie Mellon University, lorrie@cmu.edu
Ponnurangam Kumaraguru, Carnegie Mellon University, ponguru@cs.cmu.edu
Laura Mather, APWG, laura.mather@antiphishing.org
Foy Shiver, APWG, fshiver@antiphsihing.org
Peter Cassidy, APWG, APWG, pcassidy@antiphishing.org

Disclaimer: PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this message as a public service, based upon aggregated professional experience and personal opinion. These recommendations are not a complete list of steps that may be taken to avoid harm from phishing. We offer no warranty as to the completeness, accuracy, or pertinence of these recommendations with respect to any particular registrar's operation, or with respect to any particular form of criminal attack. Please see the APWG website — http://www.apwg.org — for more information. Institutional affiliations are provided for identification purposes and do not necessarily represent institutional endorsement of or responsibility for the opinions expressed herein.

Principal Investigators:
Dr. Lorrie Cranor, Associate Professor of Computer Science and Engineering & Public Policy, Carnegie Mellon University
Ponnurangam Kumaraguru, Carnegie Mellon University

Contributing Architects & Public Safety Engineers
Peter Cassidy, APWG
Foy Shiver, APWG
Nathan Yost, PHP Programming
Pat Cain, APWG
Laura Mather, APWG
Alex Bello, IronKey

Introduction and Summary

In their essential architectures of deception, there are no new confidence scams. Still the experience of electronically mediated frauds like phishing that today are animated through Internet-connected devices like PCs and handheld computers, telephones and cell phones is qualitatively different. The rise of the criminal plexus on the Internet, exploiting new forms of commerce, therefore, requires comprehensive reassessment of consumer security measures and safety education.

When ATM cards appeared in the late 1970s, financial services companies reduced much of the consumer security protocols to a single rule: no one need know the customer's Personal Identification Number (PIN), not even the bank. The rule is still in place, in part, because the delivery platform is, from a consumer's perspective, unchanged. Clearly, there'll be no facile PIN rule for this next generation of electronic commerce.

THE APWG IS COMMITTED TO PROVIDING PHISHING EDUCATION LANDING PAGES IN EVERY LANGUAGE IN WHICH PHISHING IS A SUBSTANTIVE CONSUMER OR BUSINESS THREAT

Principals of education to forearm consumers against the criminal menace gathering on the Internet, however, are beginning to emerge. One that is being illustrated in the **Phishing Education Landing Page** project, developed at the Carnegie Mellon University's **CyLab Usable Privacy and Security Laboratory (CUPS)** and the APWG, is just-in-time delivery of security instruction – presented at the moment a user exhibits a risk-laden behavior. In this instance, the risky behavior being ameliorated is the clicking of an email link to a counterfeit webpage.

The challenge of protecting consumers from frauds on the Internet is in the number of variations of schemes, media and applications abused to animate them, their speed and their fragmented nature. Breach of victim data collection and execution of cash-out events are often separated in time and in physical distance. The APWG believes penetrating experiential conditioning via just-in-time instruction has great potential for a number of security risks besides phishing and proceeds in this project with the expectation that the principal will be animated in other educational programs to modify or correct other risk-laden computer user behaviors.

Transforming a Crime Into a 'Teachable Moment'

The primary motivation of the **APWG/CMU CUPS Phishing Education Landing Page** is to instruct credulous email users the moment they have placed themselves at risk: when they have clicked on a link in a phishing email. Why? Because that failure in judgment presents a "teachable moment" for someone who has almost fallen victim of a phishing attack – and when training would be most likely to be retained and help them avoid similar dangers again. To get a sense of how it works, try it yourself, by directing your browser to: **http://education.apwg.org/r**

The logistical keystone to making the **APWG/CMU CUPS Phishing Education Landing Page** work is leveraging URLs of counterfeit websites phishers erect to fool consumers into giving them their credentials, usually in a ruse transmitted in email-based phishing attacks. When security teams have the phishing sites taken offline, usually no content is used to replace the counterfeit website at the URL deployed in the phishing email attacks.

Consumers who click on the link for a decommissioned phishing website in a phishing mail often get little more than a blank page once they arrive at the URL. [Figure 1, below.] Browser safety tools notify users of a counterfeit website – but don't provide safety instruction. CUPS and APWG posit that these cleansed URLs should be marshaled as an educational resource, substituting potent computer security education for the error messages which only confuse the most at-risk users.

Figure 1: A typical Web server error message is of little or no instructional value

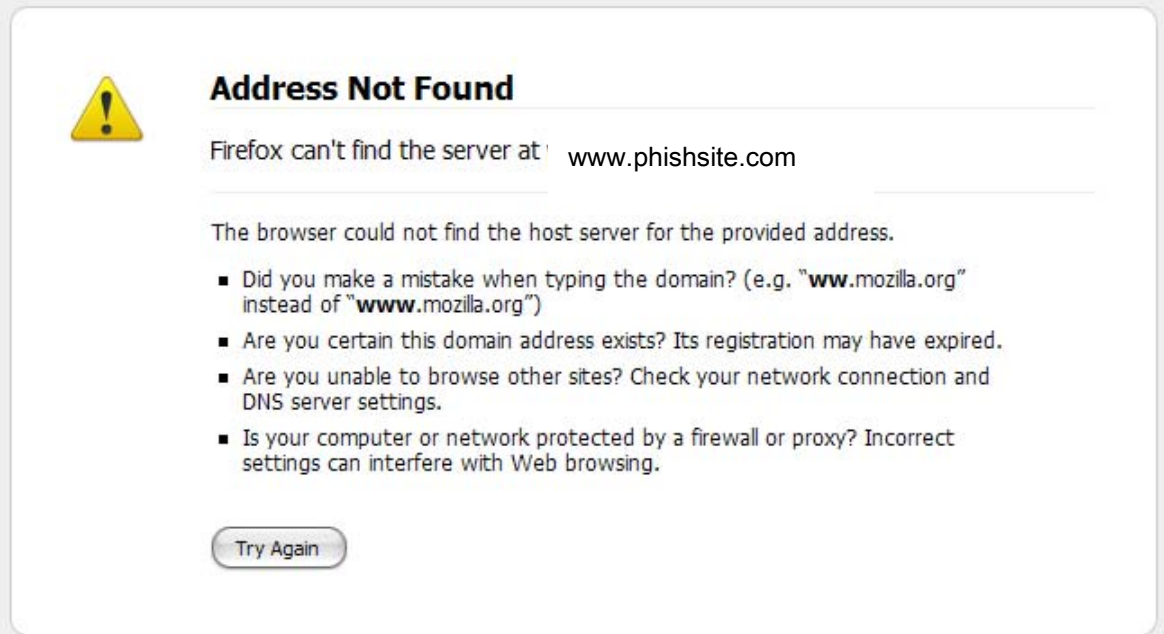


Figure 2: The Landing Page provides a clear warning and relevant safety instruction, delivered the moment a user clicks on a link in a phish mail

Carnegie Mellon's CUPS and the APWG are already repurposing URLs of decommissioned phishing Web sites through a redirect system that diverts such at-risk users to instructional materials when they have clicked the link in a phising email, just as they've identified themselves as in need of education and will be most receptive to relevant instruction to help keep them safe.

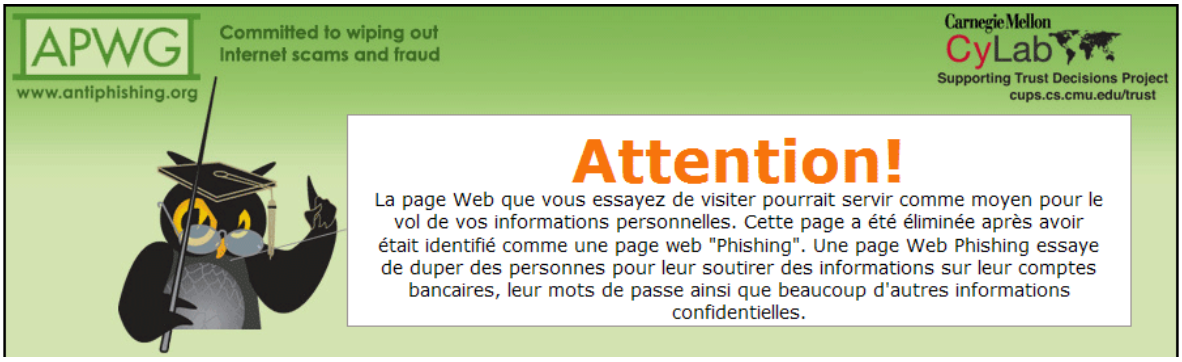
The **APWG/ CUPS Phishing Education Landing Page** provides the user with specific explanations on the event they've survived and instruction on how they can avoid being inducted into such scenarios in the future. The page warns the user that he was being inducted into a phishing scheme, tells them how the scheme worked technically and cognitively, and leaves them with a call to action to tell friends what they've learned.

The centerpiece of the landing page, however, is a set of six basic computer security and safety advisories titled "How to Help Protect Yourself" that instruct the user on such essential computer usage safety skills as:

- Developing a skeptical eye when they surf the web;
- Using good navigational habits when they visit websites or respond to unsolicited electronic correspondence;
- Learning and maintaining good computer hygiene practices.

The **APWG/CUPS Phishing Education Landing Page** has been developed and tested to be useful for the broadest consumer audience possible, with content contributions from CMU's CUPS and the APWG membership through its Internet Policy Committee (IPC), an *ad hoc* counter e-crime think tank of law enforcement, academic researchers and operations and security professionals. The deployment scenario planned would provide global coverage, with the APWG committed to providing phishing education landing pages for every language in which phishing is - or becomes – a substantive consumer or business threat.

Figure 3: Just-in-Time Phishing Education in Any Language, on Any Client Device



The APWG has already completed versions in English, French (courtesy long-time APWG member volunteer Cyveillance) and Arabic. Other versions that are in process now include German, Spanish, Bulgarian, Hebrew, Korean and Japanese. The redirect system that has been established can provide counter-phishing educational content in any language and for any client device - PCs, laptops or handhelds - that a consumer may be using when they are phished.

Phishing Education Landing Page User Experience

From the point of view of the end user, he clicks on a link in an email from a company with whom he has some relationship or interest and, suddenly, he is being admonished about the dangers of phishing by an imperious black owl waving a stick at him. To make the **APWG/CUPS Phishing Education Landing**

Page work as simply as that required some Web magic from the public safety engineers at the APWG - and a little help from the ISP community.

To make it all happen requires, first and foremost, the cooperation of the ISP whose servers were co-opted to host the phishing site. As in all phish site take-downs, the ISP administrator removes all the content of the counterfeit website associated with the URL at which the website was located. Using a redirecting utility, however, the ISP's administrators will effect an automatic redirect that will send any user attempting to navigate to the URL of a decommissioned phishing site to another URL hosted by the APWG on the APWG's own servers at: http://education.apwg.org/r

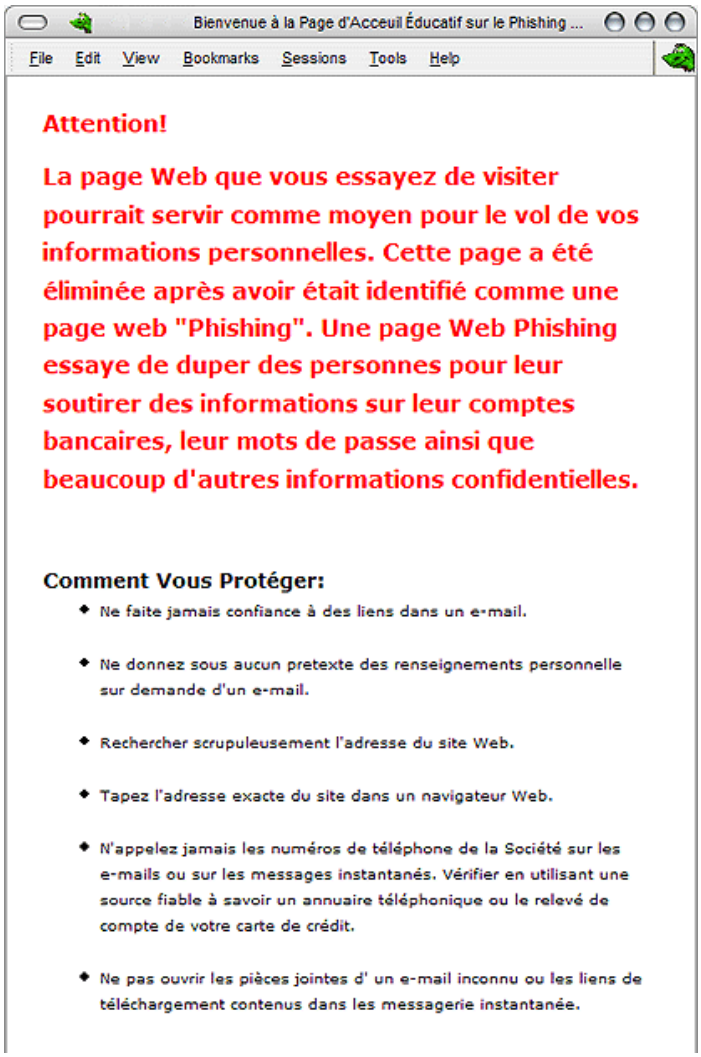


Figure 4: When the system detects a handheld browser, it renders a text page for the user, omitting the graphics of the illustrated version

Then the magic begins. The PHP system reads the Web access logs associated with the user who has been redirected to the landing page system. That information indicates the language used by the user's browser. It also relays the type of browser being employed – indicating the kind of device employed by the redirected user – a PC or laptop with full graphics capability, or a handheld device with a small form factor and limited graphic capability.

If the system detects a graphics capable PC, it will serve up a fully illustrated phishing education page. [See Figure 2 on page 5.] When the system detects a browser indicative of a handheld device, however, it will render a page exclusively of text, replicating the initial warning and the six basic security and safety advisories of the illustrated version. [See Figure 4, above left]

APWG, observing the growth worldwide in handheld computing devices and the proliferation of commerce applications that operate over them, made a design decision to assure that every device or computer redirected to the phishing education landing page would receive an immediately viewable set of computer safety instructions. In many cultures, a good deal of banking, in fact, is transacted on cell phones and other kinds of handheld devices, making this response approach an imperative in the overall system scheme.

Global Deployment Program and Development Arc

The APWG considered a number of deployment alternatives, including preparing kits that it would distribute to ISPs to self-host their own phishing education landing pages. That approach would have added distribution complexity and require a scheme to control and synchronize subsequence versions. Mounting the system locally would also require ISPs to deal with the complexities of establishing and maintaining the system.

The administrative staffs of ISPs are already stretched too thin for their own internal operations work to make demands on them. In the final analysis, the APWG concluded that the simplest solution would yield the highest degree of cooperation.

Providing a simple redirect command string to point to **http://education.apwg.org/r** was a protocol that the APWG could reasonably expect would not be rejected as an excessive demand for an already overburdened technical staff. [For technical explanation of the system and its redirect instructions, see "The Gear, the Code and All That for the Tech Ministers" on page 10.]

APWG IS SEEKING TRANSLATION PARTNERS TO PREPARE LANDING PAGE VERSIONS IN MORE LANGUAGES AND TO RECOMMEND PAGES OF LANGUAGE- AND CULTURE-SPECIFIC COMPUTER SAFETY ADVISORIES TO LINK FROM THEM

The APWG will mount versions of the **APWG/CMU CUPS Phishing Education Landing Page** in any language for which there is a standardized text-encoding format that can be rendered by a standard browser. The APWG is actively seeking translation partners to 1) prepare versions in more languages and 2) to provide links to language- and culture-specific computer safety and security advisories that link off of the phishing education landing page, providing further instruction. The APWG provides its own sponsoring members the opportunity to co-brand versions of the landing page.

Cognitive Aspects of Just-in-Time Computer Safety Instruction

Foremost among the challenges faced by interveners who wish to provide PC safety instruction is the experiential conditioning to which consumers are regularly exposed, often contravening widely accepted computer usage safety guidelines. One APWG research fellow in 2005 reported that no generally accepted Web surfing safety rule had *not been broken* one way or another by industry itself, usually by way of the marketing department, well and truly foreclosing on any meaningful industrial dialog about broader educational and safe-usage conventions. Any rule drafted would be broken as a matter of course the moment it was adopted.

THE APWG BELIEVES EXPERIENTIAL CONDITIONING VIA JUST-IN-TIME DELIVERY OF SAFETY INSTRUCTION HAS GREAT POTENTIAL FOR A NUMBER OF SECURITY RISKS BESIDES PHISHING

To counter this, CUPS and the APWG established the landing pages in order to provide an experiential mechanism to train at-risk consumers in counter-phishing skills. The content of the landing page is based on the PhishGuru cartoons developed at CUPS. CUPS researchers observed in user studies that users were ignoring security alert emails sent by companies, but were spending time reading phishing messages.

The researchers decided to try sending users simulated phishing messages and displaying anti-phishing training when users clicked on the links and fell for the phish. This "embedded training" approach worked extremely well. The researchers experimented with a variety of different types of training messages, and after several rounds of iteration arrived at a cartoon format featuring the PhishGuru goldfish character[1] [Kumaraguru, et. al 2006].

The cartoon format leverages a number of instructional design principles from learning science by providing a story line with characters to tell the story and illustrations integrated with the textual content [Clark 2002].

In laboratory studies, the CUPS research team discovered that the PhishGuru cartoon effectively educated users who saw it after falling for a fake phish, but was completely ineffective when delivered directly in the body of an email. Thus, by

[1] The PhishGuru goldfish character is a trademark of Wombat Security Technologies, Inc.

leveraging the "teachable moment" researchers were able to engage users and motivate them to pay attention [Kumaraguru et al., 2007].

In a follow-up field study, the research team demonstrated that the PhishGuru embedded training approach is an effective way for companies to train their employees to avoid phishing attacks [Kumaraguru, et al. 2008]. In a large real-world study involving Carnegie Mellon University students, faculty, and staff, participants remembered what they learned a month after training [Kumaragru, et al. 2009].

The **APWG/CUPS Phishing Education Landing Page** works on the same principles as embedded training by leveraging the teachable moment when people fall for real phishing attacks at websites that have already been taken down. Thus, training is delivered to the people who are most susceptible to phishing attacks at the moment when they are likely to be most receptive to training.

The Gear, the Code and All That for the Tech Ministers

To animate the Phishing Education Landing Page, the APWG is requesting that instead of disabling phish sites, ISP, registrars, and other infrastructure entities put an HTTP redirect in place of the phishing page at the phishing URL.

In addition, by including a parameter (the URL of the decommissioned phishing website) within that redirect script, co-operating correspondents will also help the APWG and CMU's Supporting Trust Decisions Project track the success rates of the various phishing education campaigns.

This is invaluable information and we appreciate your cooperation in including this parameter in the redirect URL. Your efforts can help educate consumers and enterprise computing users so that they can better protect themselves from electronic crime.

Implementing a Redirect in Apache

There are several ways to implement a redirect in Apache, but the following method is one of the simplest.

1. Create a .htaccess file in the directory where the phishing site was stored. Note the leading dot on the .htaccess filename.

2. The .htaccess file should contain the following text:

   Redirect 301 /the-phishing-page.html
   http://education.apwg.org/r/en?www.phishsite.com/the-phishing-page.html
   (In the above text, "the-phishing-page.html" should be replaced with the filename of the phishing webpage that was taken down and "www.phishsite.com/the-phishing-page.html" should be replaced by the full URL of the phish site that was taken down. Note that there are two things that need to be replaced by the full URL of the phish site. For example, "the-phishing-page.html" could be "signin.html" and "www.phishsite.com/the-phishing-page.html" could be "yourcompany.com/update/signin.html")

3. The .htaccess file should be owned by an unprivileged "utility" user and group, and set to be world readable and writable by no one.

   More information about .htaccess files can be found here:
   http://httpd.apache.org/docs/2.2/howto/htaccess.html

Implementing a Redirect in Internet Information Server (IIS)

To redirect to the APWG/CMU education URL in IIS, change the HttpRedirect property for the resource to:

http://education.apwg.org/r/en?the-phishing-page.html, PERMANENT

Note that "the-phishing-page.html" should be replaced with the filename of the phishing webpage that was taken down. For example, "the-phishing-page.html" could be "signin.html."

More information on IIS redirects can be found here:
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/b652c863-6334-40be-8a97-db4b368f3ecc.mspx?mfr=true

References

Clark, R. C. and R. E. Mayer. 2002. *E-Learning and the science of instruction: proven guidelines for consumers and designers of multimedia learning*. Jossey-Bass/Pfeiffer.

P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M.A. Blair, and T. Pham. School of Phish: A Real-Word Evaluation of Anti-Phishing Training. CyLab Technical Report: cmu-cylab-09-002, March 2009.http://www.cylab.cmu.edu/research/techreports/tr_cylab09002.html

P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. Cranor and J. Hong. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. Proceedings of the 2nd Annual eCrime Researchers Summit, October 4-5, 2007, Pittsburgh, PA, p. 70-81.http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf

P. Kumaraguru, Y. Rhee, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In CHI 2007: Conference on Human Factors in Computing Systems, San Jose, California, 28 April - May 3, 2007, 905-914. http://doi.acm.org/10.1145/1240624.1240760

P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong.Lessons from a real world evaluation of anti-phishing training. In *Proceedings of the third eCrime Researchers Summit (eCrime 2008)*, October 15-16, 2008, Atlanta, GA. http://www.cs.cmu.edu/~ponguru/eCrime_APWG_08.pdf