APWG/CyLab Phishing Education Landing Page

The APWG/Carnegie Melon CyLab Phishing Education Landing Page (Landing Page) is designed to instruct Internet users about online safety at the "most teachable moment": when they have just clicked on a link in a phishing communication attempting to trick them into to sharing personal information.

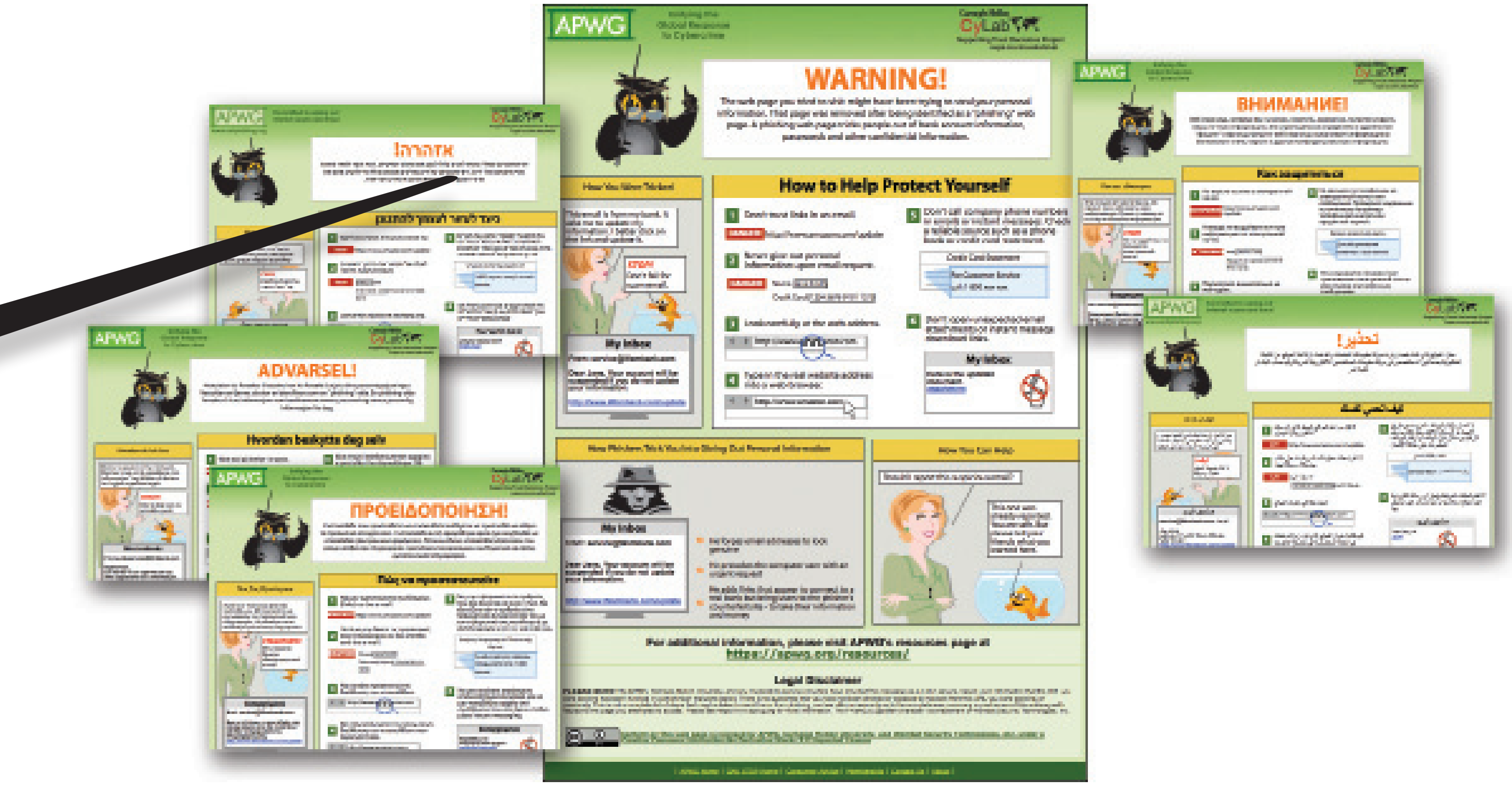
Once a hosting provider identifies and decommissions a phishing website, its managers set up the redirect to **education.apwg.org/r**. The Landing Page system does the rest, by handling web requests from users and answering in one of 21 languages after interrogating the language setting of the users' browsers.

By current usage estimates, the Landing Page serves tens of thousands of the credulous per month - at no cost to the users it protects or infrastructure managers who conspire with the APWG to transform phishing websites into educational resources for the most at-risk users.

How the APWG Phishing Education Landing Page Magic Works

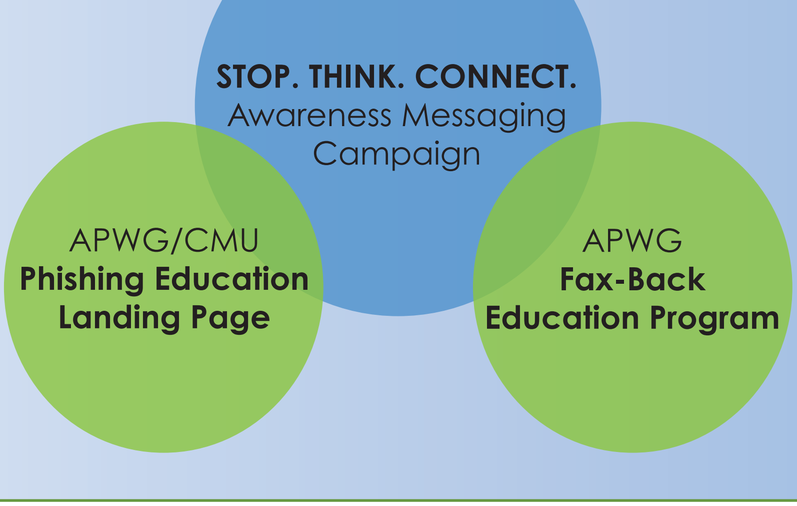
The APWG Internet Policy Committee and Carnegie Mellon Cylab Usable Privacy and Security Laboratory (CUPS) created and tested a webpage to educate users about phishing. As part of the process for shutting down a phishing website, APWG is asking ISPs and web hosting managers to intercept users from accessing decommissioned phishing websites and redirect them to the Phishing Education Landing Page a http://education.apwg.org/r

Once a user's browser resolves the terminal web destination, the Landing Page explains that the user has just been victimized by a phishing scam (though email or other hyper-linked media), and advises both consumers and enterprise users about the ways they can protect themselves and avoid being victimized in the future.


APWG
CyLab
WARNING!
How to Help Protect Yourself
My Inbox
For additional information, please visit APWG's resources page at https://apwg.org/resources/
Legal Disclaimer
ВНИМАНИЕ!
!אזהרה
ADVARSEL!
Hvordan beskytte deg selv
ΠΡΟΕΙΔΟΠΟΙΗΣΗ!
!تحذير

APWG Public-Health Model of Counter-Cybercrime Intervention

Real-time interventions for at-risk users who click on phishing links and answer fax-based frauds, combined with the ubiquitous messaging of the global **STOP. THINK. CONNECT.** campaign effect the most effective behavior-modifying approach possible, reinforcing best practices broadly while individually instructing the most at-risk users to adopt better online habits.



STOP. THINK. CONNECT.
Awareness Messaging Campaign

APWG/CMU
Phishing Education Landing Page

APWG
Fax-Back Education Program

Easy Steps for Hosting Providers to Redirect Traffic From Retired Phishing Websites to the Landing Page

Implementing a redirect in Apache

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

The .htaccess file should contain the following text:

Redirect 301 /the-phishing-page.html http://education.apwg.org/r/?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”)

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 IIS

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

http://education.apwg.org/r/?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

Life Cycle

Most of the damage from an online phishing attack is inflicted in the first hours of a phishing campaign. Still, given the store-and-forward logistics of email, unknowing users can still fall victim over time (think “long-tail”). For that reason, APWG requests hosting providers make the redirects active for as long as practical and allowed given house policies.

If you would like to learn more about this initiative, please contact APWG at info@apwg.org.