Fax Back Phishing Education Program

The APWG Fax Back Phishing Education Program (APWG Fax Back), is a keystone of the APWG's global public education programs to provide freely available alerting and educational instruments to help Internet users be more secure in all of their online activities.

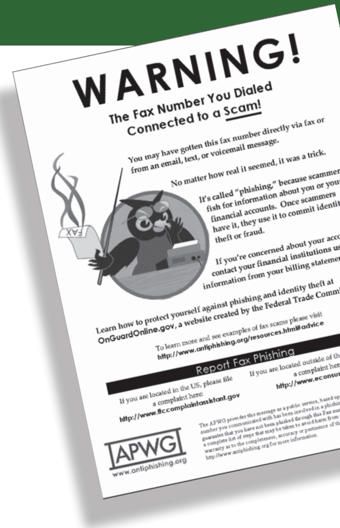
In tandem with APWG's education redirection program for email-based Phishing scams, APWG Fax Back provides 1) effective interdiction and 2) educates the most likely victims of fax-based scams so they can better protect their privacy and financial accounts.

Fax scams mimic "official" communications with logo and letterhead from government agencies and businesses, transmitted by email (with a return fax number) or faxes (with a return fax number in the coversheet), to fool people into revealing personal information to fraudsters. The goal of APWG Fax Back is to instruct users at a "teachable moment," when they've fallen victim to a scam requesting data on personal or financial accounts.

How APWG Fax Back Magic Works

Working with Fax-over-Internet (FoIP) providers, fax server hosting companies, and ISPs, anytime a user sends a fax reply to a hosted fax number of a known scam, the Fax Back program:

1. Intercepts, receives and destroys the victim's fax containing the personal information
2. Determines the victim's fax number(s) from Caller ID data or from Call Detail
3. Faxes the APWG Fax Back education page back to the victim's fax to alert them of the malicious nature of the communication, and directs them to online resources to report additional suspicious messages or to see examples of common fax and email scams so they can more easily identify them in the future.



WARNING!

The Fax Number You Dialed Connected to a Scam!

You may have gotten this fax number directly via fax or from an email, text, or voicemail message.

No matter how real it seemed, it was a trick.

It's called "phishing," because scammer fish for information about you or you financial accounts. Once scammers have it, they use it to commit identit theft or fraud.

If you're concerned about your acc contact your financial institutions us information from your billing statemen

Learn how to protect yourself against phishing and identity theft at OnGuardOnline.gov, a website created by the Federal Trade Commi

To learn more and see examples of fax scams please visit
http://www.antiphishing.org/resources.html#advice

Report Fax Phishing

If you are located in the US, please file a complaint here:
http://www.ftccomplaintassistant.gov

If you are located outside of th a complaint here
http://www.econsu

APWG
www.antiphishing.org

The APWG provides this message as a public service, based up number you communicated with has been involved in a phishin guarantee that you have not been phished through this Fax num a complete list of steps that may be taken to avoid harm from warranty as to the completeness, accuracy or pertinence of thi http://www.antiphishing.org for more information.

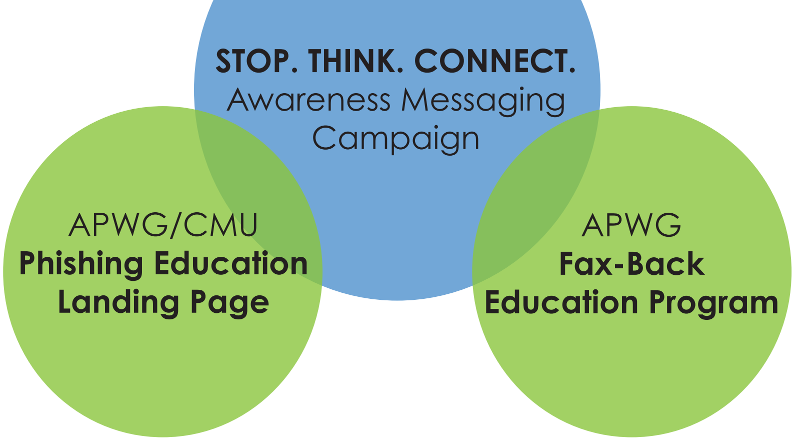
How APWG Fax Back Can Work For Your Agency Or Brand

To initialize the Fax Back system for a specific attack, a victimized brandholder and/or their responders first need to determine the telco or service provider managing the fax service hosting the co-opted telephone number being exploited for a fax-based phishing campaign.

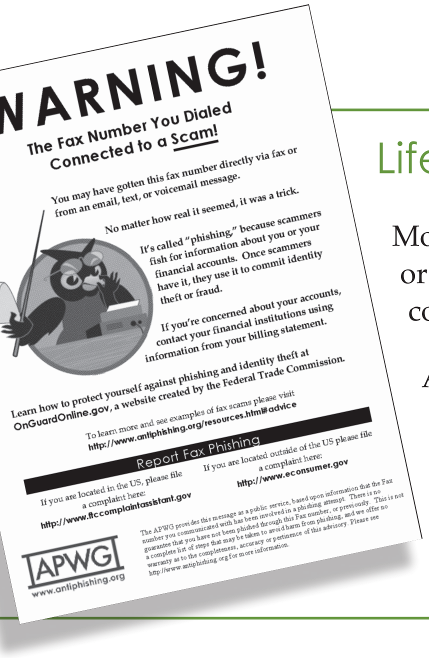
1. Public resources like Telcodata.us and Fonefinder.net can point to managing telcos and cybercrime responder services can draw from industry resources to find the parties authorized to set up a fax-back routine.

2. FoIP providers, fax server hosting companies and ISPs need only download the APWG instructional Fax Back page in PDF or TIFF format and ready it for transmission back to customers who send information to "blacklisted" fax numbers utilized for fax-based scams.

3. With that, the managers can set their server scripts to invoke the APWG Fax Back education page and send a copy of the the cover sheet to a credulous user attempting to send in their data to a once compromised fax number.


STOP. THINK. CONNECT.
Awareness Messaging Campaign
APWG/CMU
Phishing Education Landing Page
APWG
Fax-Back Education Program

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 potent and effective behavior-modifying approach possible, reinforcing best practices broadly while individually instructing the most at-risk users to adopt better online habits



WARNING!

The Fax Number You Dialed Connected to a Scam!

You may have gotten this fax number directly via fax or from an email, text, or voicemail message.

No matter how real it seemed, it was a trick.

It's called "phishing," because scammers fish for information about you or your financial accounts. Once scammers have it, they use it to commit identity theft or fraud.

If you're concerned about your accounts, contact your financial institutions using information from your billing statement.

Learn how to protect yourself against phishing and identity theft at OnGuardOnline.gov, a website created by the Federal Trade Commission.

To learn more and see examples of fax scams please visit **http://www.antiphishing.org/resources.html#advice**

Report Fax Phishing

If you are located in the US, please file a complaint here: **http://www.ftccomplaintassistant.gov**

If you are located outside of the US please file a complaint here: **http://www.econsumer.gov**

The APWG provides this message as a public service, based upon information that the Fax number you communicated with has been involved in a phishing attempt. There is no guarantee that you have not been phished through this Fax number, or previously. This is not a complete list of steps that may be taken to avoid harm from phishing, and we offer no warranty as to the completeness, accuracy or pertinence of this advisory. Please see http://www.antiphishing.org for more information.

APWG
www.antiphishing.org

Life Cycle

Most of the damage in an online phishing attack is inflicted in the first 8 hours or so. Tying up a fax line for more than a few days, therefore, would be counterproductive and costly to an enterprise already running on thin margins.

APWG requests that, for consumer benefit and minimal disruption to FoIP providers and fax server hosting companies' enterprises that these response scripts be kept live for one week before the number is released to normal customer use.

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

APWG Public-Health Model of Counter-Cybercrime Intervention

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