# The State of Internet Fraud and Crime and Useful Attempts to Battle the Miscreants

Foy Shiver
Deputy Secretary-General
APWG

# APWG Institutional Profile

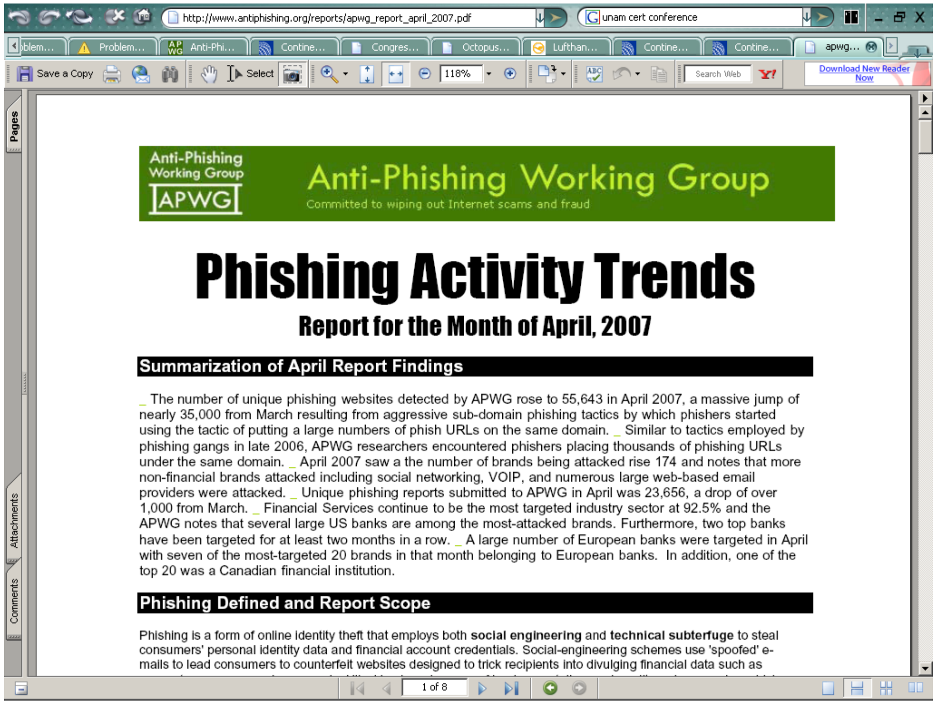
- Over 3000 members from almost 1800 companies, government and private agencies world wide
- Membership restricted to:
  - Financial institutions
  - ISPs
  - E-commerce sites
  - Law enforcement agencies
  - Government agencies
  - Technology companies
  - Research partners (CERTs, Universities, Labs, Volunteer Organizations)
  - Consumer groups

# APWG Institutional Profile

- Founded October 2003
  - Independently incorporated, 501c6 tax exempted association, directed by its directors, executives, steering committee, members and correspondent research partners
- **Mission**: Provide resources for information and solutions for eliminating the fraud, identity theft and electronic crime that result from phishing, pharming and email spoofing of all types
  - Initially focused on phishing, broadening focal length to include phraud and ecrime
  - Clearinghouse of ecrime data being developed on modified biomedical research model – open access; governed usage through user agreements

# Institutional Roles: Statistician

- APWG Phishing Activity Trends reports delineate the phishing experience, enumerating phishing's growth and characterizing phishing's evolution to inform stakeholder dialog
  - Monthly reports cover social engineering phishing attacks and crimeware threats
    - Developing: report segment on electronic crime infrastructure



Anti-Phishing Working Group
APWG

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud

Phishing Activity Trends

Report for the Month of April, 2007

**Summarization of April Report Findings**

_ The number of unique phishing websites detected by APWG rose to 55,643 in April 2007, a massive jump of nearly 35,000 from March resulting from aggressive sub-domain phishing tactics by which phishers started using the tactic of putting a large numbers of phish URLs on the same domain. _ Similar to tactics employed by phishing gangs in late 2006, APWG researchers encountered phishers placing thousands of phishing URLs under the same domain. _ April 2007 saw a the number of brands being attacked rise 174 and notes that more non-financial brands attacked including social networking, VOIP, and numerous large web-based email providers were attacked. _ Unique phishing reports submitted to APWG in April was 23,656, a drop of over 1,000 from March. _ Financial Services continue to be the most targeted industry sector at 92.5% and the APWG notes that several large US banks are among the most-attacked brands. Furthermore, two top banks have been targeted for at least two months in a row. _ A large number of European banks were targeted in April with seven of the most-targeted 20 brands in that month belonging to European banks. In addition, one of the top 20 was a Canadian financial institution.

**Phishing Defined and Report Scope**

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as

# Institutional Roles: Advisor

APWG has contributed data to the OCC, FDIC, European Commission, ITU, Congressional committees, ICANN, law enforcement agencies, government agencies and law courts worldwide

# Institutional Roles: Mustering Point

– Three Established Conferences Each Year

– Association where stakeholders meet and pull together projects of stakeholder benefit

- Data and technology projects draw contributions from industry, academe, law enforcement and standards-making communities
- ICANN Policy Project
- Abuse Manager Contact Federation Project Under Way

APWG MEMBER

www.antiphishing.org

Annual General Members Meeting

eCRS for academic and industrial research into eCrime

Deloitte.

ECIJA

MarkMonitor

RSA
The Security Division of EMC

S21sec

CeCOS for responders to eCrime events & managers of end-users' security

# eCrime Maintains a Steady Pace

- Little change over the past year
  - Quantity continues to increase
  - More coordinated “inside” jobs and targeted attacks
  - As the big boys get their acts together criminals focusing on smaller targets that are not prepared
- Economic downturn seems to promote an increase in a “safe” crime
  - Desperate people resorting to desperate acts
  - More availability of easier tools
  - Experienced criminals focus on Job scams and Muling recruitment
  - Many seem to see it as a Victimless crime

# APWG Strategic Contributions to Counter-eCrime Efforts

The eCrime Fighters Gather at the Front

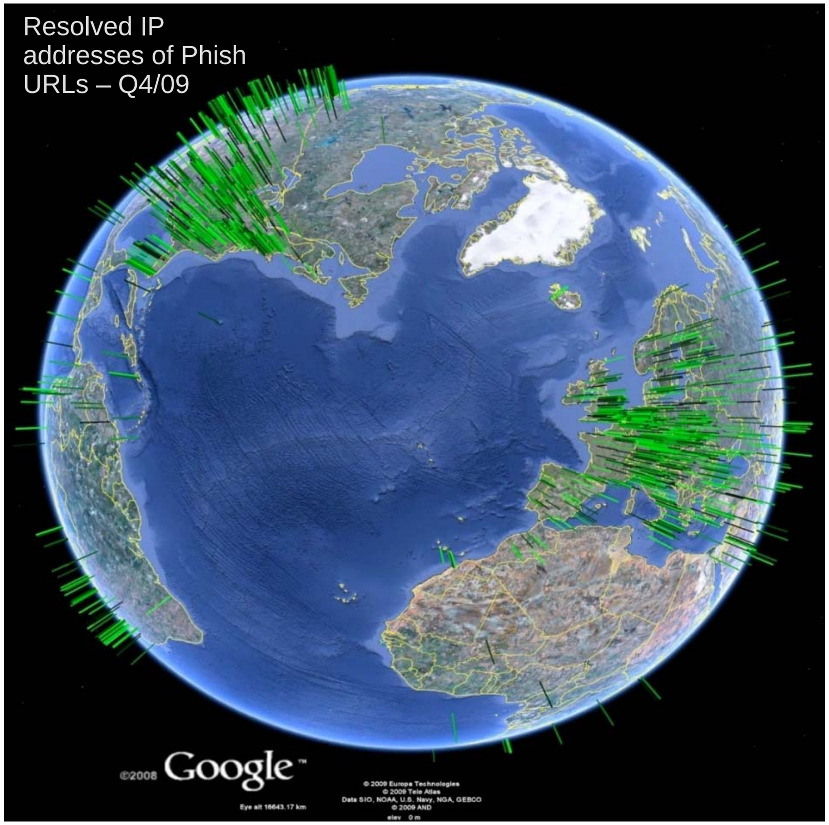
# Phishing Attack Repository & URL Block List

## APWG Phishing Attack Data Repository

3 Million + historical records of phishing events and related data

## Phishing Attack URL Block List (UBL)

- Updated every 5 minutes; listing of previous 72 hours attacks with URLs
- Used to power warning systems in browsers and tool bars
- Inform signaling systems for security teams
- Inform research and development of counter-eCrime technology



Resolved IP addresses of Phish URLs – Q4/09

# Repository & Block List

- Repository and Block List Users
  - 129 agencies, companies and associations taking outbound feed
  - 60 agencies and companies making inbound contributions
  - A number of university researchers examining the full repository for research purposes
- Repository and Block List Sources
  - Brand holders send confirmed URLs directly to the Repository
  - APWG member security and take-down companies send confirmed URLs directly to the Repository
  - Reportphishing@antiphishing.org - unconfirmed reports to APWG for processing
    - Automated parsing pulls out relevant data and places it in Block list
  - Volunteer organizations (PIRT and PhishTank)
  - Research partners

# Repository & Block List (cont)

- Multiple uses in counter-ecrime technologies and forensics
  - Integrated browser anti-phishing systems
  - Standalone toolbars
  - Industrial research and development
  - University research
  - eCrime forensic analyses
- Why It’s Working and Will Continue to Grow
  - Clearinghouse model operates similarly to the genomic databases used by life sciences researchers in the US and Europe
  - Assurance that the full resource available will be provided
  - User agreement that assigns no new liability
    - Role of NDAs, User Agreements often underappreciated in technical community
- New contributing companies, groups and associations coming online regularly

# More Tools

- One of our central missions is to get people to play nice together.
- You're aware of our XML-based sharing formats. (IODEF)
- ~1 year ago, "we" volunteered to help with tools
  - Not getting any "we need this tool…"
  - We started writing tools that sounded good
  - http://sourceforge.net/projects/ecrisp-x/

# Need an eCrime Reporting Standard

- Industry research concluded there is no good way to electronically report fraud activities
  - No common format
  - Good reports need complete data sets
  - Reports need to support automatic processing
- Goals
  - Make it easy to spot and report novel events & trends
  - Let vendors & researchers test their ideas/products against known attacks
  - Be vendor and application agnostic
  - Try not to reinvent another format
  - Pick something acceptable to CERTs, ISPs, law enforcement and bank teams
- IETF Incident Object Description and Exchange Format (IODEF) XML schema (with eCrime-relevant extensions)
  - Flexible (simple through detailed)
  - Easy to read
  - Standard-brand XML, immediately useable

# IODEF Extensions XML Schema for eCrime Reporting

Extensions to the IODEF-Document Class for Phishing, Fraud, and Other Crimeware

- Structured data model allows forensic searches and investigations to be automated/scripted with greater ease using standard schema
  - Multiple language capability
  - Reports readable in any XML-capable browser
  - Multiple parties – brandholders; security professionals, CERT personnel and LE - can add to a report
  - Extensions specifically designed for electronic crime incidents and crimeware
    - Purpose built nature gives it unique relevance
- XML makes reports readable by people and assists in the editing of ecrime reports, adding data & organizing human-driven workflows

# The Evidence Collection Project

- The APWG volunteered to set up a project on evidence collection, full of little sub-projects:
  - What data is included
  - How to send it, share it, etc
  - How does this work legally
  - Format for the data

# Evidence Collection Project (2)

- The currently planned tasks:

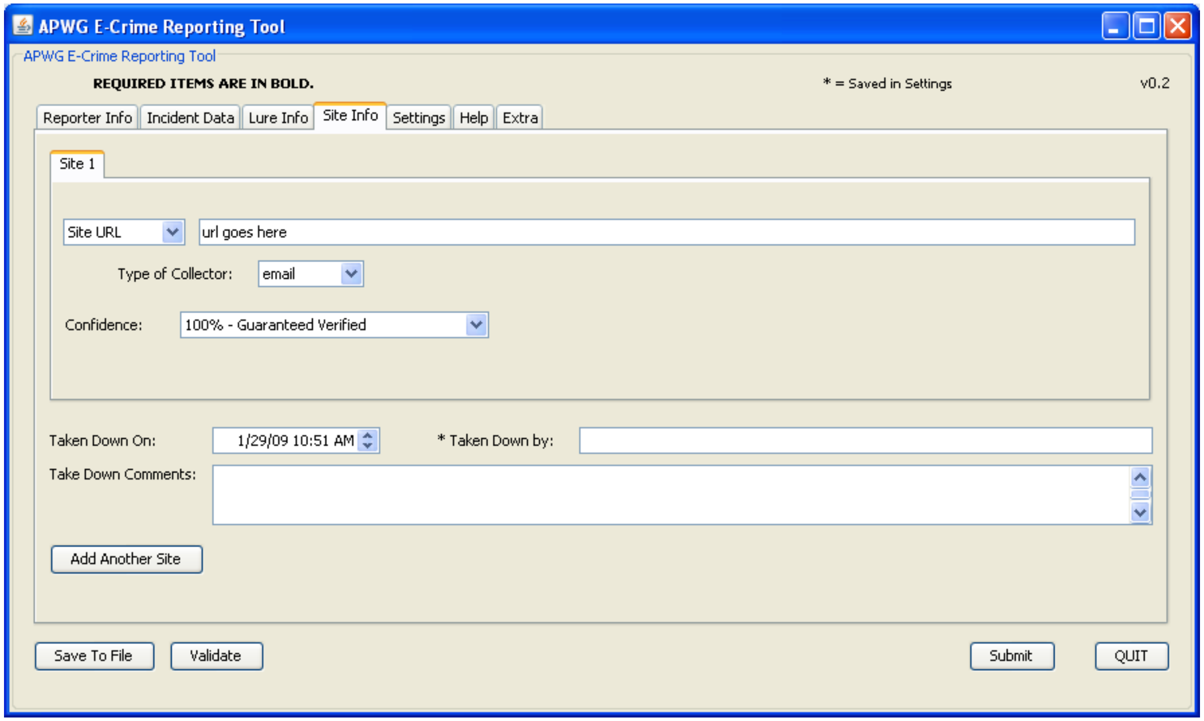
1. Do a broad call (CFI) to see if such a document(s) exists.
2. Develop advisory(ies) on what to grab, how to grab, how to process, etc, when doing evidence collection.
3. Publish advisory; receive impolite comments.
4. Revise and publish a second version.

# ECP (3) – aka EColle

- The target audience is system admins, LEs & ISPs
- The hope is to keep the working team small
- Target completion is 2009

- The "CFI" should go out soon
- If you wish to participate, contact us
- If you've solved this problem… come tell us

# APWG eCrime Reporting Tool



REQUIRED ITEMS ARE IN BOLD.

* = Saved in Settings

v0.2

Site URL: url goes here

Type of Collector: email

Confidence: 100% - Guaranteed Verified

Taken Down On: 1/29/09 10:51 AM

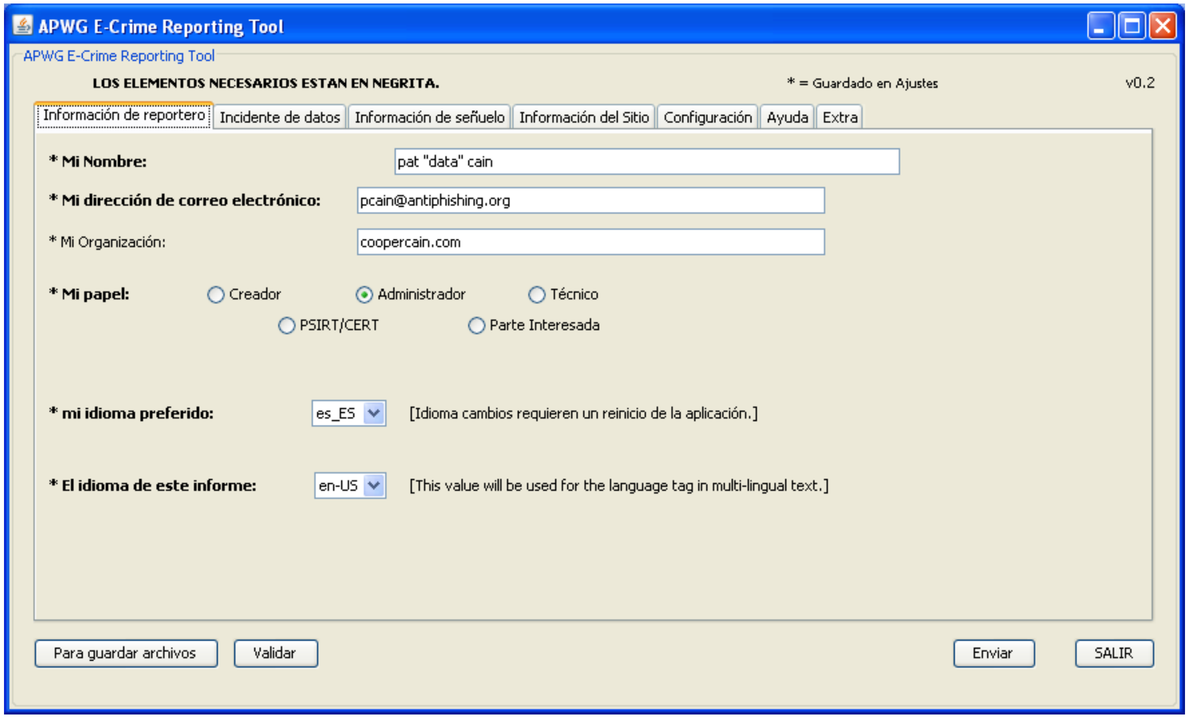
* Taken Down by:

Take Down Comments:

Java-based eCrime Reporting Tool console runs on any machine that plays Java. Simple interface allows anyone to make out a report by stepping through and populating tabbed templates. A network engineer can use it. More importantly, a local cop with minimal technical vocabulary can use it

Working betas established for US-EN, UK-EN and ES-ES (Spain-native Spanish.) More languages to come. **Goal**: create eCrime Reporting Tool available in every language in which electronic crime is a problem to help establish and feed private sector, public sector and non-profit eCrime data repositories

# APWG eCrime Reporting Tool



**LOS ELEMENTOS NECESARIOS ESTAN EN NEGRITA.** * = Guardado en Ajustes v0.2

*** Mi Nombre:** pat "data" cain

*** Mi dirección de correo electrónico:** pcain@antiphishing.org

* Mi Organización: coopercain.com

*** Mi papel:** ○ Creador ● Administrador ○ Técnico ○ PSIRT/CERT ○ Parte Interesada

*** mi idioma preferido:** es_ES [Idioma cambios requieren un reinicio de la aplicación.]

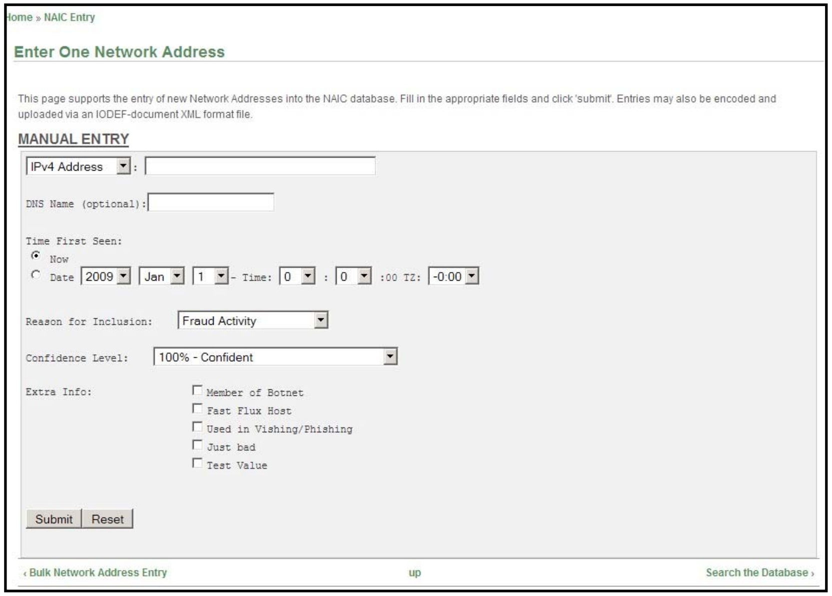
*** El idioma de este informe:** en-US [This value will be used for the language tag in multi-lingual text.]

The APWG eCrime Reporting Tool assures complete reports are made and are written to a universally readable and writable XML format. Console can be set for local filing, remote or third-party repository filing or submission directly to the APWG repository

**Next Step**: Creation of open souce tools to translate data souces into IODEF Extensions format to mobilize now islanded data of forensic value

# APWG Network Address Intelligence Clearinghouse

- Network Address Intelligence Clearinghouse (NAIC), a members' only, limited-access database to archive network addresses specifically tied to an electronic crime event or an instance of attempted or successful fraud
- Different from URL Block List which archives location of sites; focus is on network address location of cash-out attempts or account-hacking activities – from telephone numbers to Internet Protocol (IP) addresses



Home » NAIC Entry

Enter One Network Address

This page supports the entry of new Network Addresses into the NAIC database. Fill in the appropriate fields and click 'submit'. Entries may also be encoded and uploaded via an IODEF-document XML format file.

MANUAL ENTRY

IPv4 Address ▾ :

DNS Name (optional):

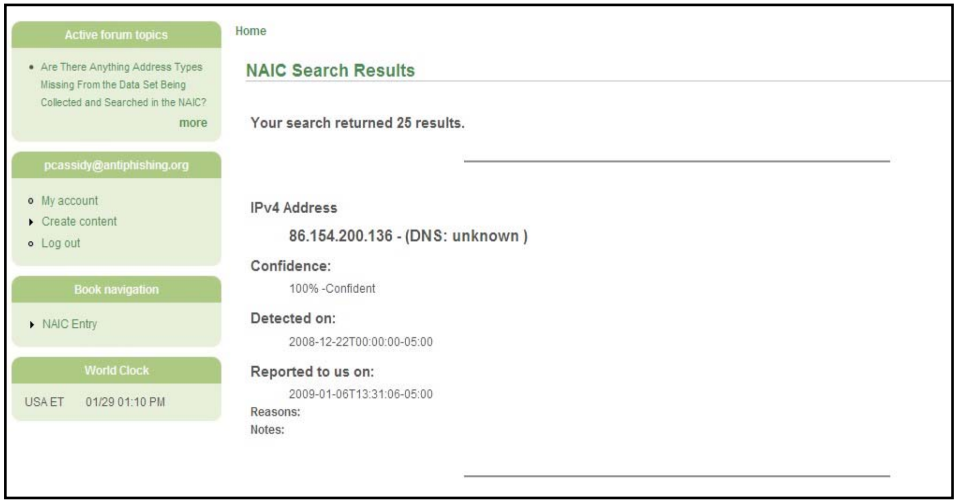
Time First Seen:
● Now
○ Date 2009 ▾ Jan ▾ 1 ▾ - Time: 0 ▾ : 0 ▾ :00 TZ: -0:00 ▾

Reason for Inclusion: Fraud Activity ▾

Confidence Level: 100% - Confident ▾

Extra Info:
□ Member of Botnet
□ Fast Flux Host
□ Used in Vishing/Phishing
□ Just bad
□ Test Value

Submit
Reset
‹ Bulk Network Address Entry
up
Search the Database ›



Active forum topics
Are There Anything Address Types Missing From the Data Set Being Collected and Searched in the NAIC?
more
pcassidy@antiphishing.org
My account
Create content
Log out
Book navigation
NAIC Entry
World Clock
USA ET 01/29 01:10 PM
Home

NAIC Search Results

Your search returned 25 results.

IPv4 Address
86.154.200.136 - (DNS: unknown )

Confidence:
100% -Confident

Detected on:
2008-12-22T00:00:00-05:00

Reported to us on:
2009-01-06T13:31:06-05:00

Reasons:

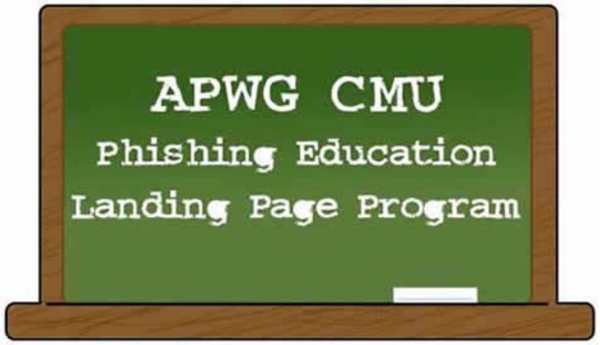
Notes:

# Emergent Law Enforcement-Network Security Initiative (eLENS)

- A concerted effort to bridge the gap between public law enforcement, private network security, investigative intelligence, network measurement and experimentation, and related ***policy***.
- We see the operational lines between these entities blurring, there is no corresponding policy to guide and coordinate what is occurring informally and on an ad hoc basis.
- Initial goal is to develop and promote uniform data exchange guidelines that address the full life cycle of information flows: discovery, acquisition, sharing, and disclosure.
- Focus on the legality of capturing, observing and sharing network activity, including the proper roles of the various stakeholders, and observance of evidentiary chain-of-custody principles to ensure resulting actions are ethically and legally actionable.
- We see ecrime law enforcement evolving toward a model more similar to public health initiatives (WHO) in the way the data is collected, collated and analyzed to determine remedial action required

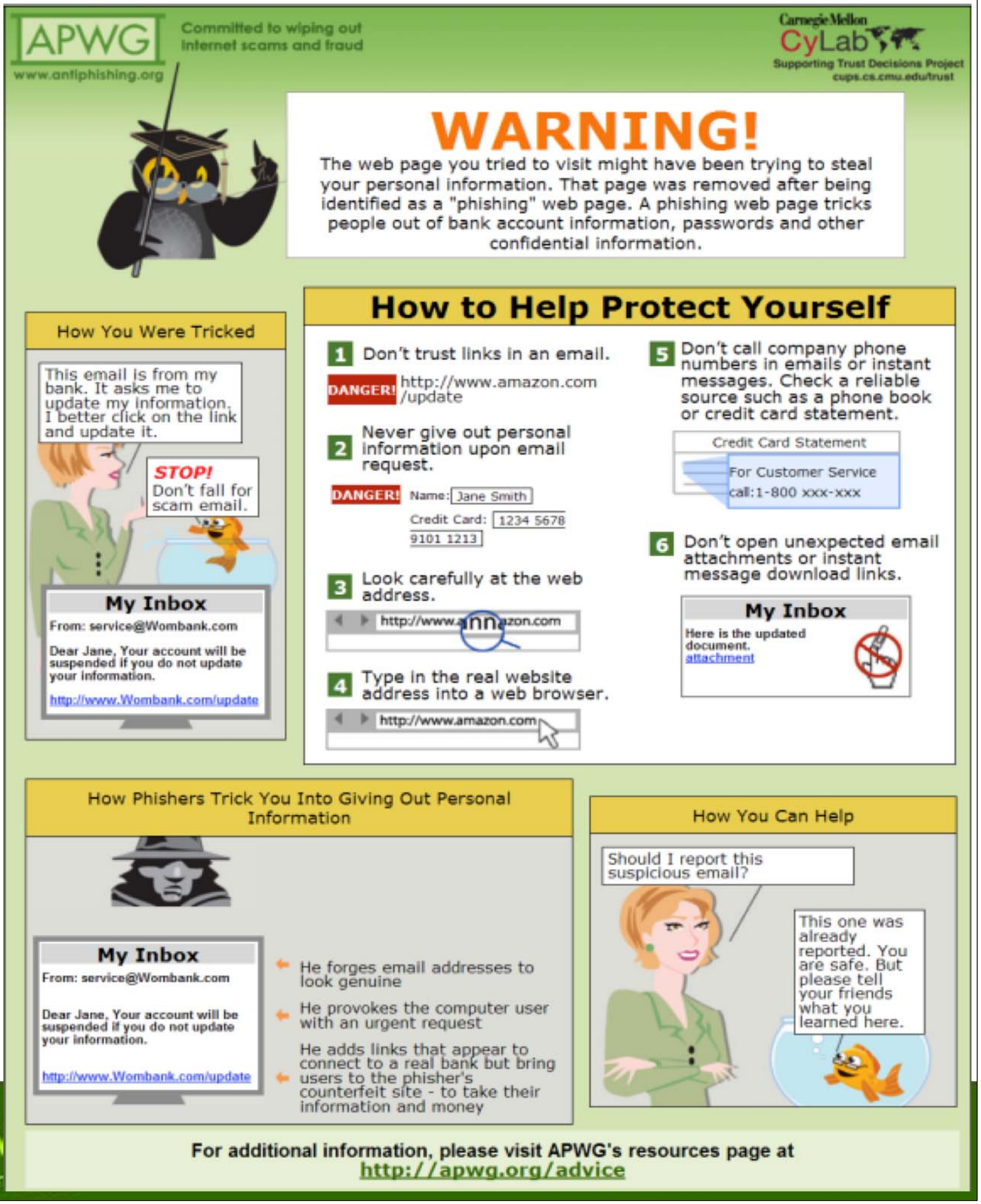
# APWG/CMU Education Redirect Page

- A multi-language APWG Hosted site used to educate users when they follow a known phishing link



- ISPs replace phish site content with an auto-redirect that brings the consumer to the education page. The system parses language and browser and delivers appropriate version of the page to the user
- The landing pages instruct consumers on online safety at the “most teachable moment”: when they have just clicked on a link in a phishing communication
- Co-Branding Available

# Redirection Landing Page



APWG Committed to wiping out internet scams and fraud www.antiphishing.org

Carnegie Mellon CyLab Supporting Trust Decisions Project cups.cs.cmu.edu/trust

## 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. It asks me to update my information. I better click on the link and update it.

STOP! Don't fall for scam email.

**My Inbox**

From: service@Wombank.com

Dear Jane, Your account will be suspended if you do not update your information.

http://www.Wombank.com/update

### How to Help Protect Yourself

1 Don't trust links in an email.

DANGER! http://www.amazon.com/update

2 Never give out personal information upon email request.

DANGER! Name: Jane Smith Credit Card: 1234 5678 9101 1213

3 Look carefully at the web address.

http://www.amnazon.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-xxx

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

**My Inbox**

Here is the updated document. attachment

### How Phishers Trick You Into Giving Out Personal Information

**My Inbox**

From: service@Wombank.com

Dear Jane, Your account will be suspended if you do not update your information.

http://www.Wombank.com/update

- He forges email addresses to look genuine
- He provokes the computer user with an urgent request
- He adds links that appear to connect to a real bank but bring users to the phisher's counterfeit site - to take their information and money

### How You Can Help

Should I report this suspicious email?

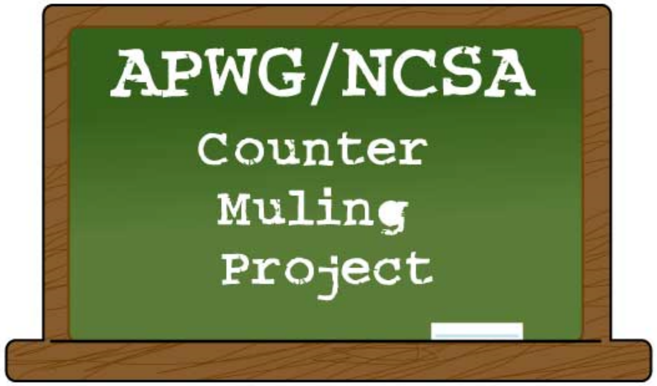
This one was already reported. You are safe. But please tell your friends what you learned here.

For additional information, please visit APWG's resources page at http://apwg.org/advice

# APWG/NCSA Counter-Muling Project

- The Counter Muling Project development team is a joint effort of the APWG and the National Cyber Security Alliance (NCSA)
- Tasked to develop a series of video podcasts for distribution among our membe companies and agencies, research partners, government agencies, trade and law enforcement associations and traditional electronic media

  **Message**: Muling is a crime, whether you are fooled or not; here's how to avoid it
- A number of electronic educational instruments are being developed, to be delivered in broad media campaigns and in a just-in-time modality like the APWG/CMU Phishing Education Landing Page Program which delivers counter-phishing



# Working Group Initiatives

- Fast-Flux Working Group Report
  - APWG working with ICANN's SSAC have released their initial study on fast flux

  http://www.icann.org/en/announcements/announcement-26jan09-en.htm

- ICANN domain tasting
  - ICANN requested comments on domain tasting
  - DNSPWG submitted comments on how phishers don't appear to use domain tasting, but that domain tasting still impacts the anti-phishing efforts

  http://www.apwg.com/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

- ICANN IDNs
  - ICANN requested comments on Internationalized Domain Names (IDNs)
  - Drafted best practices on how IDNs can be implemented without impacting the anti-phishing community

# Working Group Initiatives (cont)

- Registrar Best Practices
  - Provide a set of recommendations to the domain registrar community that can substantially reduce the risk and impact of phishing on consumers and business worldwide
  - Focus on 3 areas where registrars can be of assistance: Evidence Preservation for Investigative Purposes, Proactive Fraud Screening and Phishing Domain Takedown
  - http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
- I have been hacked FAQ
  - Targeted at web site owner or operator who suspects, discovers, or receives notification that it's web site is being used to host a phishing site
  - Covers important response measures to take in the areas of identification, notification, containments, recovery, restoration and follow-up

    http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf

# Working Group Initiatives (cont$^2$)

- Request for participation on creating new gTLDs
  - ICANN is doing additional research on creating new gTLDs
  - Looking for insight to reduce consumer confusion and likelihood of fraud/cybercrime
- Accelerated Domain Suspension Plan
  - IPC members have written a proposal for registries to suspend domains that are being solely used for phishing
  - Need to finalize an arbitration process for contesting a suspension and a take-down provider accreditation process
  - .asia is committed to being the first to roll-out the plan  
    .mx and others are looking and interested in the program
- PBL? – Phone number/SMS addresses

# Some Other Closed Initiatives

- SubDomain Study out
  - "*Making Waves in the Phisher' Safest Harbors: Exposing the Dark Side of Subdomain Registries*"
  - How phishers now use what we call subdomain registries to provide safe harbors for malicious and criminal activities
  - Measures individuals and organizations can consider if they opt to make these harbors less attractive and effective to phishers

  http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

- ICANN WhoIS Proposal
  - Discussion to remove access to WhoIs data
  - APWG provided operational insight on how DNS and WHOIS data are exploited
  - Highlighted role of the DNS in different kinds of Internet-mediated crime
  - Proposal had been basically dropped until further research can be conducted

# Thank You

Foy Shiver

fshiver@antiphishing.org

+1 404.434.7282