The Anti-Phishing Working Group: Electronic Crime, Fraud 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, email spoofing and malicious software of all types
    - Initially focused on phishing, broadening focal length to include fraud and ecrime
    - Clearinghouse of ecrime data being developed on modified biomedical research model – open access; governed usage through user agreements
    - Promote research to fight electronic crime of all types

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

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

APWG MEMBER
www.antiphishing.org

Annual General Members Meeting

e-Crime Researchers Summit
APWG

eCRS for academic and industrial research into eCrime

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
  - More sophisticated malicious software and scareware
- 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

Electronic Crime is Different

- Forensic narrative in eCrime is most often elusive:
  - Never as easy as 'guy robbed a bank and fled on foot, south on Main St.'
- Forensic practices well established and time tested for conventional crime – not so eCrime
- Data voluminous and largely redundant
  - Human processing made impossible by overwhelming volume of data and disparate file formats
- Data scattered across disparate jurisdictions and venues
  - Disparate data protection laws complicate collection, sharing and processing of eCrime data
  - Industry and academic researchers, holding large proportion of forensically potent data are left under a cloud of legal uncertainty and exchange more *ad hoc* than formally

LE Agrees Cooperation is Key to Success of LE Effort

- Lot of Cooperation between national law enforcement agencies and between local and national agencies
  - Recent US/Egypt Phish Phry Busts
  - Multinational LE efforts growing in scope and success

Council of Europe Cybercrime convention

- A multilateral convention will ensure that all States Parties:
- Cooperate in investigating criminal activities and in providing usable evidence for prosecutions;
- Provide a 7/24 Point of Contact

QUESTION: But what would LE and industry-stakeholder cooperation require to respond as fast as the electronic crimes are committed, a truly contemporaneous response?

Data Mobilization for Machine Processing of eCrime Event Data

- Optimal eCrime Response: Automation of the recruitment and machine processing of eCrime event data for forensic applications

Optimal eCrime Event Data Mobilization requires:

Common terminal file formats for archive and exchange of eCrime data

Formal corresponding exchange and usage agreements to govern access to - and use of - the archived eCrime data

Formally governed clearinghouses of eCrime event data for private industry professionals and public agency law enforcement personnel engaged in forensic enterprise

APWG Strategic Contributions to Counter-eCrime Efforts

The eCrime Fighters Gather at the Front

eCrime Event Data Clearinghouses for Industry

- Clearinghouse model forces examination of data usage and related liability issues in private sector
  - Success: URL Block List (UBL) archives 30,000-50,000+ records per month
  - Clearinghouse success owes a lot of governance innovation established by APWG in user agreement
  - The technology was the easy part
  - Creation of a formal trust relationship between users of the clearinghouse users took work

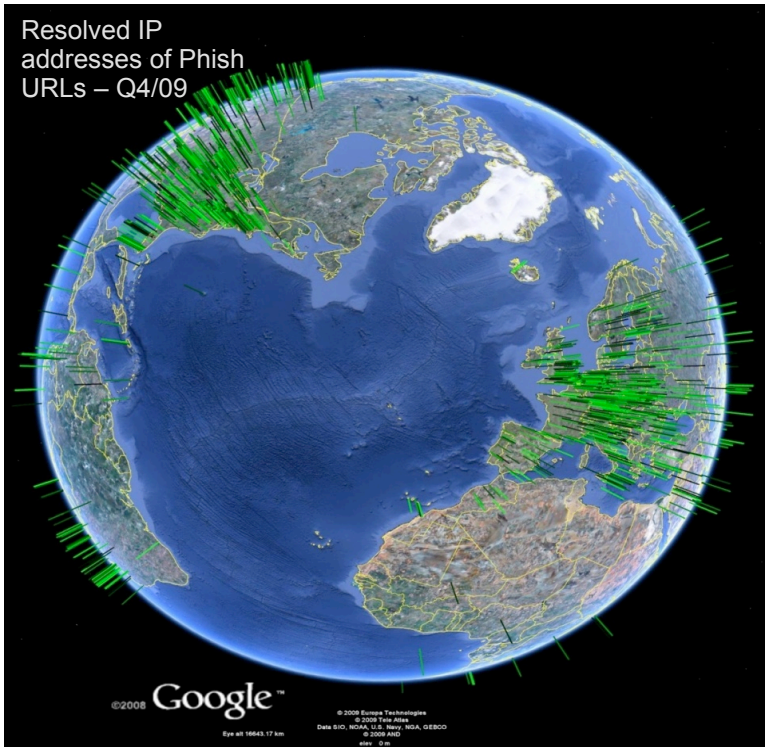
Phishing Repository& URL Block List

APWG Phishing Attack Data Repository

5 Million + historical records of phishing events and related data

Phishing URL Block List (UBL)

- Updated every 5 minutes; listing of previous 72 hours attacks with URLs
- Informs browser warning systems and anti-phishing tool bars
- Signaling systems for security teams
- Informs research and development of counter-eCrime technology
- 60 signatories from CERTs, brand-holders, telecom companies, security companies and software developers



Key Factor to Success of UBL: Liability Management Model

- 2003-2005 companies tried to establish commercial data clearinghouses
- Agreements attempted to isolate liability, so that that reporters were liable for their correctness, giving subscribers recourse for faulty data
- Caused friction for contributors: unknown - and growing liability - as subscribers came onto the network
- Agreements would take months of legal negotiations - and abandoned
- APWG took another tack: contractual framework of mutual indemnification. Publishers and exchange bear no liability for correctness
- Data is scored with confidence factors based on data source, their historical accuracy, and level of pre-submission vetting
- Data has different applications depending on the confidence factor
- All parties, subscribers and publishers, have exactly same agreement, with the same indemnification and liability clauses

Challenge: 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

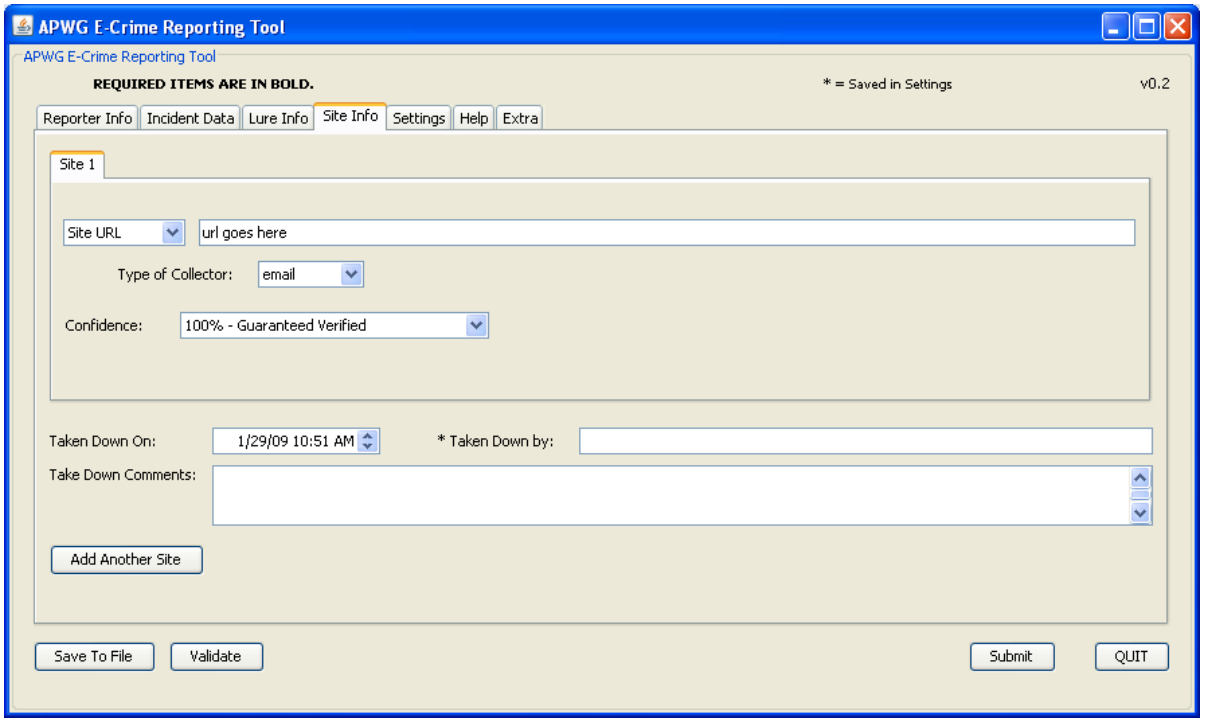
IODEF Extensions XML Schema for eCrime Reporting

- 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

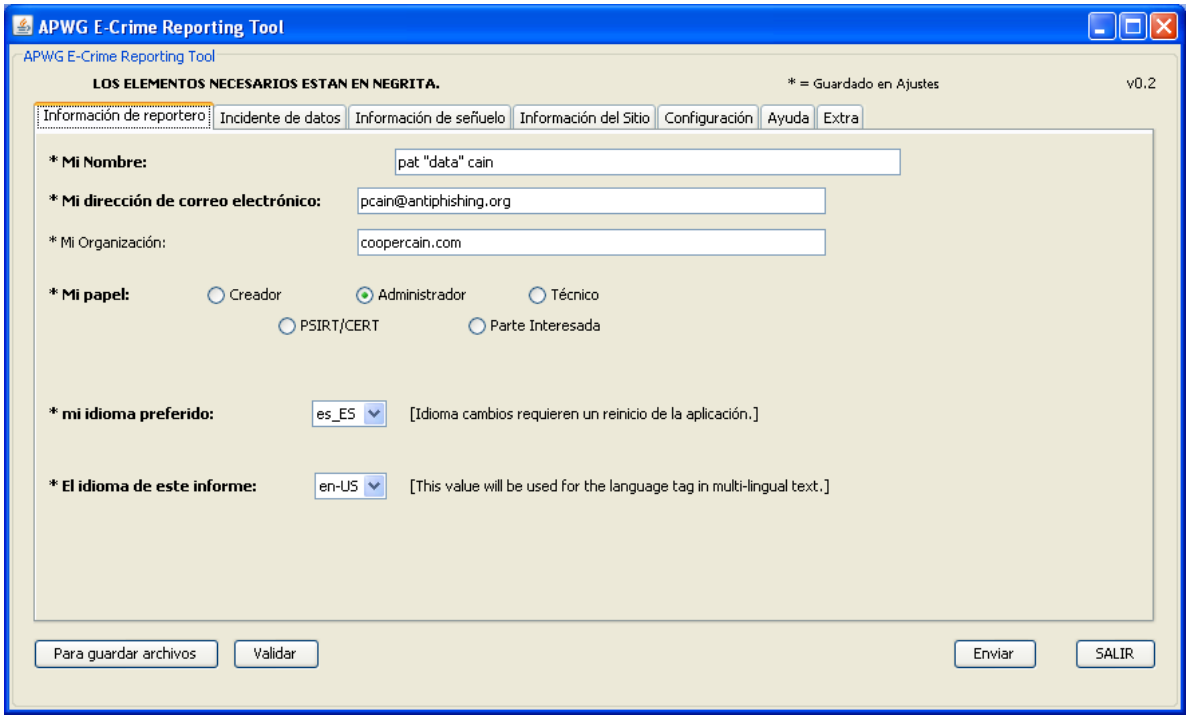
APWG eCrime Reporting Tool



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

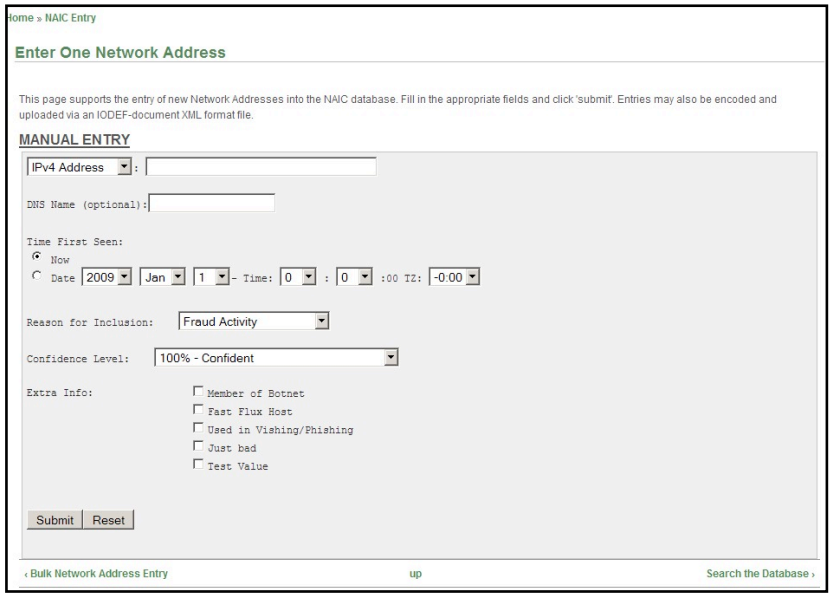


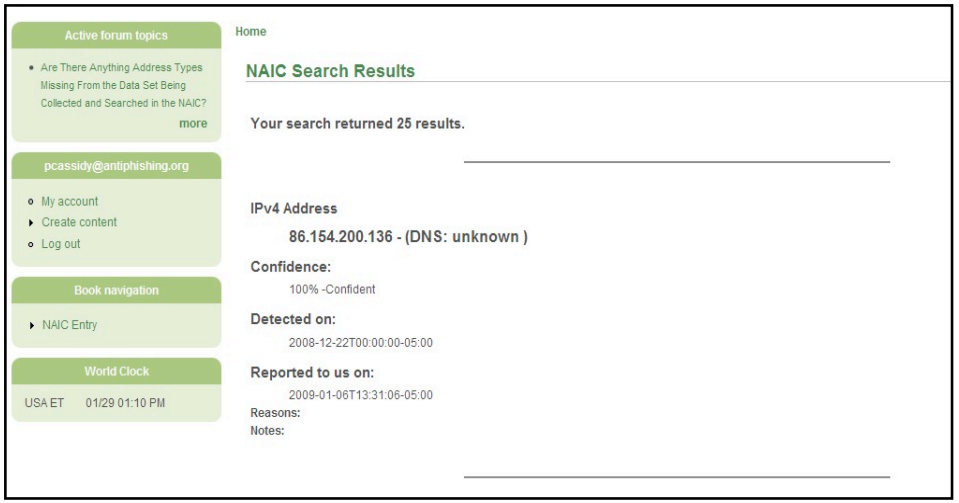
The APWG eCrime Reporting Tool assures complete reports are made and are written to a universally readable and writable XML format. Console can be set for local filing, remote or third-party repository filing or submission directly to the APWG repository

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





APWG Accelerated Domain Suspension Program

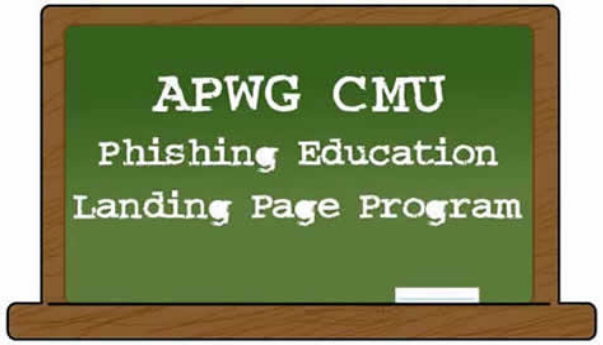
- Created a proposal for registries to suspend domains that are being solely used for phishing
- Need to finalize an arbitration process for contesting a suspension and a take-down provider accreditation process
- Will provide an interface and credentials for reporting and tracking malicious domains
- Several TLDs are ready to implement when ready.
- Beta version should be available for testing in Q2

APWG Education Initiatives

- Education Redirect Page
- Counter-Muling eduction
- Consumer Messaging Forum

APWG/CMU Education Redirect Page

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



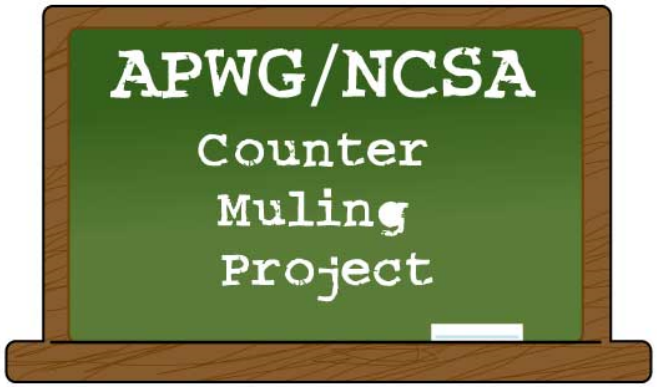
- ISPs replace phish site content with an auto-redirect that brings the consumer to the education page. The system parses language and browser and delivers appropriate version of the page to the user
- The landing pages instruct consumers on online safety at the "most teachable moment": when they have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

Redirection Landing Page

APWG/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



Online Consumer Security and Safety Messaging Convention

- Developing a public-awareness online security and safety message and/or messaging suite
- Goal is a single, simple message for consumers to remember for online security and safety
- Message can be used to build a framework for other actionable safety and security measures consumers can take in different areas of the Internet
  - ecommerce
  - social networking
  - banking

New Working Group Initiatives

- Registration Abuse Working Group
- Study on vulnerabilities for hacking web servers to put up phishing sites
- 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

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

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