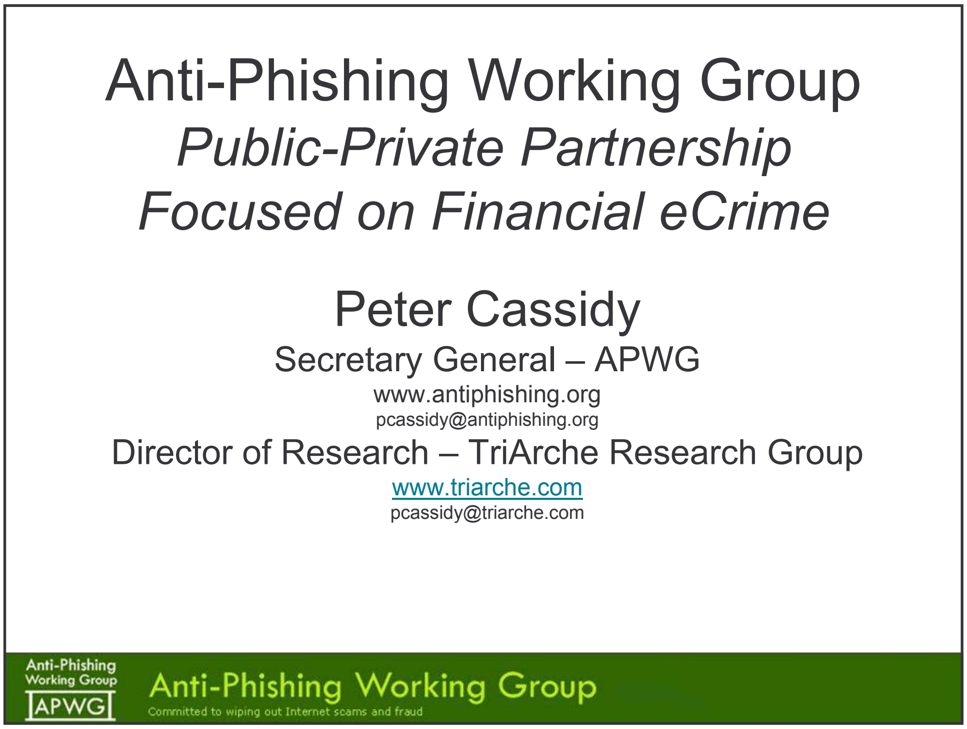


Anti-Phishing Working Group

Public-Private Partnership Focused on Financial eCrime

Peter Cassidy

Secretary General – APWG

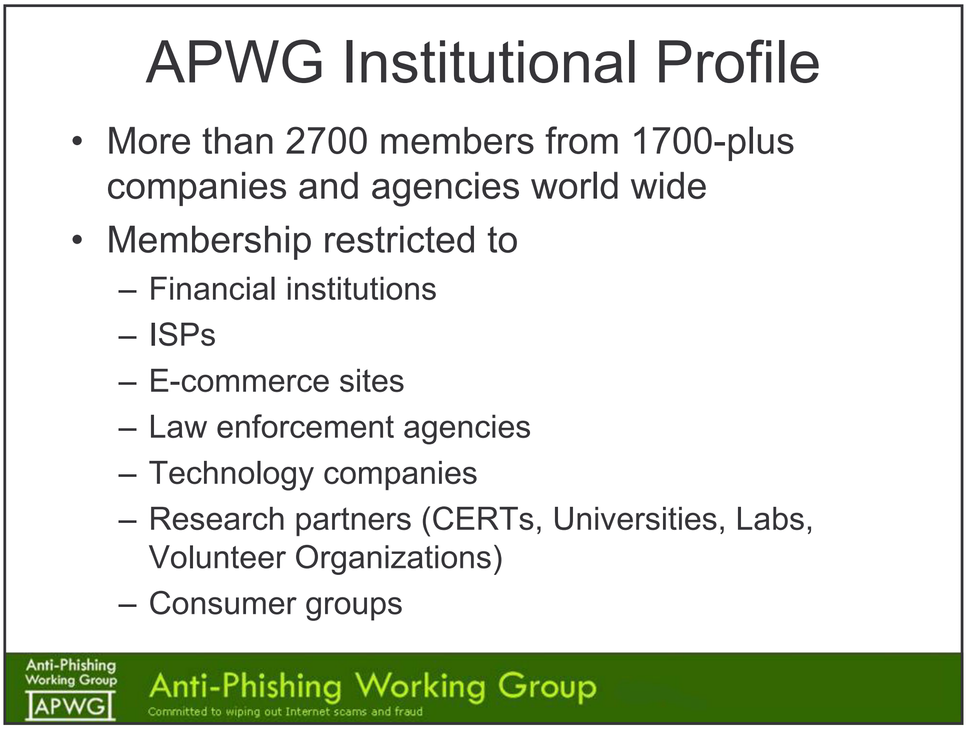
www.antiphishing.org

pcassidy@antiphishing.org

Director of Research – TriArche Research Group

www.triarche.com

pcassidy@triarche.com



APWG Institutional Profile

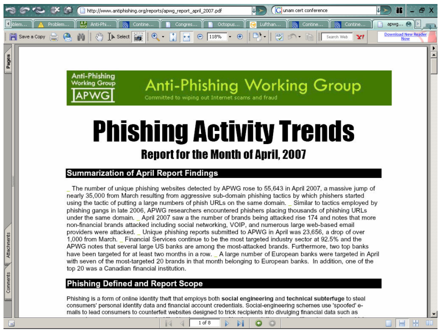
- More than 2700 members from 1700-plus companies and agencies world wide
- Membership restricted to
  - Financial institutions
  - ISPs
  - E-commerce sites
  - Law enforcement agencies
  - Technology companies
  - Research partners (CERTs, Universities, Labs, Volunteer Organizations)
  - Consumer groups

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**: Maintaining a federating nexus to organize counter-ecrime stakeholding community and neutral, third-party clearinghouses of data for forensic applications
  - 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



http://www.antiphishing.org/reports/apwg_report_april_2007.pdf

unam cert conference

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

Phishing Activity Trends

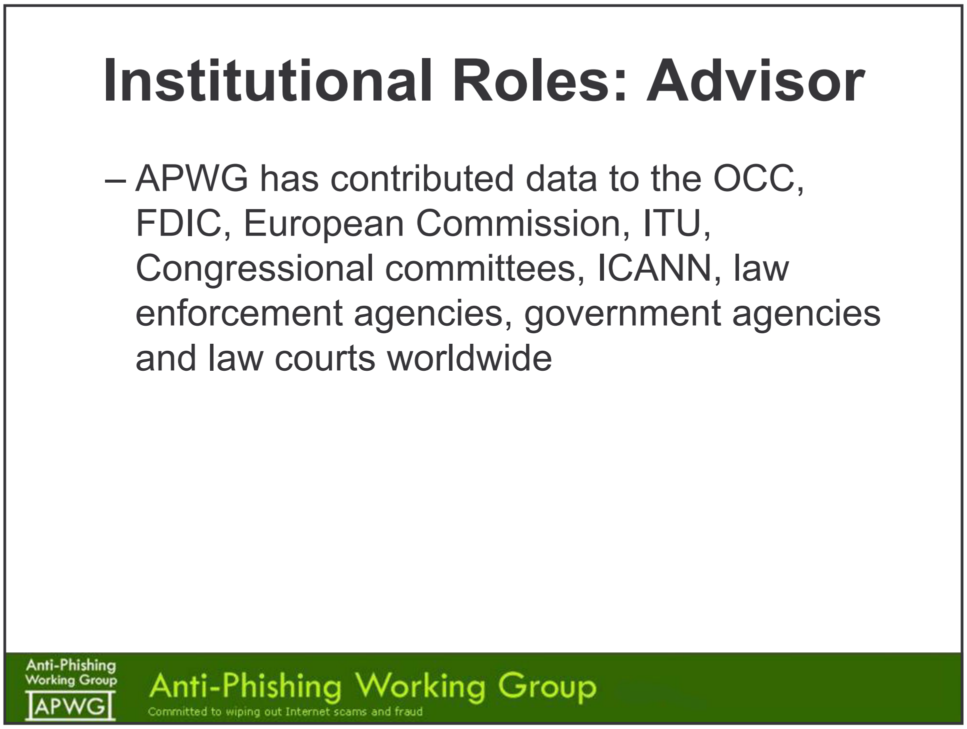
Report for the Month of April, 2007

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

– 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

– Three Established Conferences

Anti-Phishing Working Group APWG
e-Crime Researchers Summit APWG
APWG Counter-eCrime Operations Summit
May 30 & 31
San Francisco

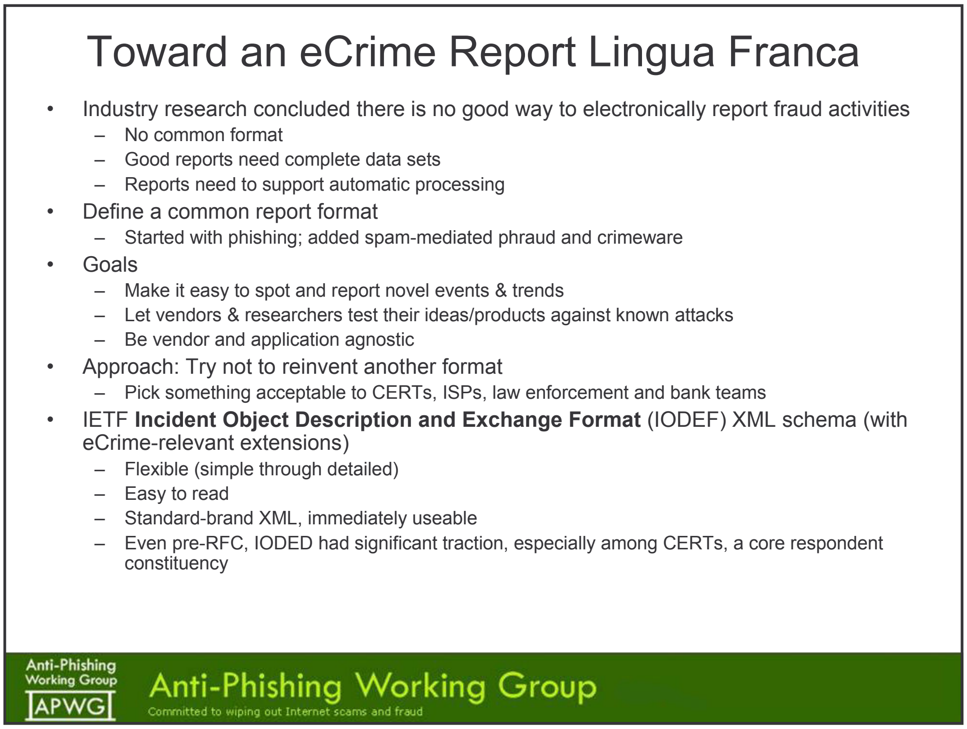
Annual General Members Meeting

eCRS for academic and industrial research into eCrime

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

APWG Strategic Contributions to Counter-eCrime Efforts

Toward an Electronic Crime Reporting Lingua Franca



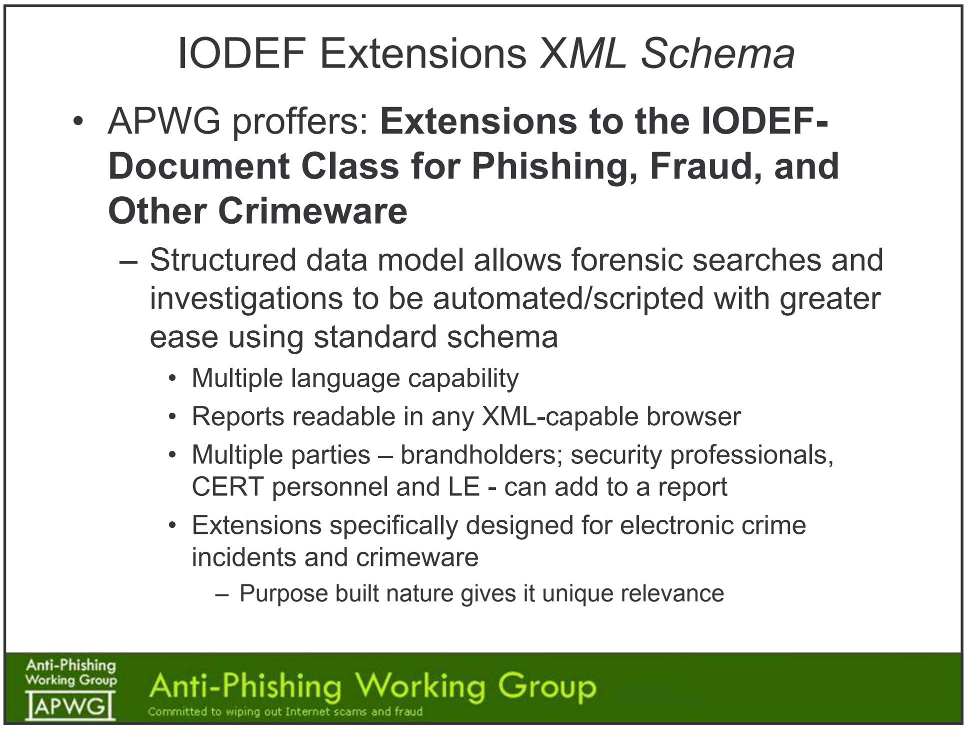
Toward an eCrime Report Lingua Franca

- 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
- Define a common report format
  - Started with phishing; added spam-mediated phraud and crimeware
- 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
- Approach: 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
  - Even pre-RFC, IODED had significant traction, especially among CERTs, a core respondent constituency

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud



IODEF Extensions X*ML Schema*

- APWG proffers: **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

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

From Raw Phish Mail to Reports

From: support@coopercain.com
Sent: Friday, June 10, 2005 3:52 PM
To: pcain@coopercain.com
Subject: You have successfully updated your password
Attachments: updated-password.zip

Dear user pcain,
You have successfully updated the password of your Coopercain account.
If you did not authorize this change or if you need assistance with your account, please contact Coopercain customer service at: support@coopercain.com

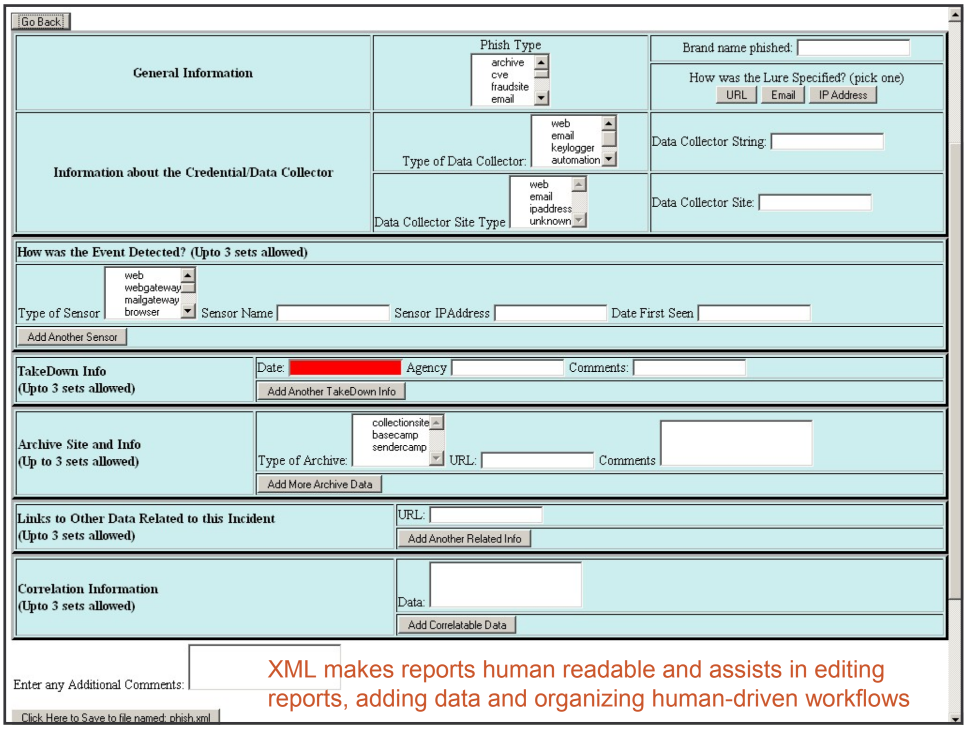
Thank you for using Coopercain!
The Coopercain Support Team

+++ Attachment: No Virus (Clean)
+++ Coopercain Antivirus - www.coopercain.com

Example Report in XML Schema

```
<IODEF-Document.>
<Incident purpose="other">
   <IncidentID Issuer="Pat">PAT2005-06</IncidentID>
   <Description>This is a test report from actual data.</Description>
   <Contact contacttype="person" contactrole="creator">
        <NameIdentifier format="emailAddress">pcain@coopercain.com</NameIdentifier>
   </Contact>
   <ReportTime>2005-06-22T08:30:00-05:00</ReportTime>
   <Assessment> <Confidence rating="high" /> </Assessment>
   <EventData>
    <DetectTime>2005-06-21T18:22:02-05:00</DetectTime>
    <AdditionalData dtype="xml">
      <PhraudReport FraudType="" Version="" xmlns="phish">
       <FraudParameter>Subject: You have successfully updated your password</FraudParameter>
       <FraudedBrandName>Cooper-Cain</FraudedBrandName>
       <LureSource> <Address iodef:addrcat="ipv4-addr" iodef:spoofed="unknown">
<Addr>216.231.63.162</Addr>
            </Address>   </LureSource>
        <OriginatingSensor OriginatingSensorType="human">
           <Address iodef:addrcat="ipv4-addr"> <Addr>10.0.0.4</Addr>  </Address>
        </OriginatingSensor>
```

XML makes reports machine readable and assists in making processing automated – and programmable



Go Back

General Information	Phish Type archive cve fraudsite email	Brand name phished: How was the Lure Specified? (pick one) URL Email IP Address
Information about the Credential/Data Collector	Type of Data Collector: web / email / keylogger / automation	Data Collector String:
	Data Collector Site Type: web / email / ipaddress / unknown	Data Collector Site:

How was the Event Detected? (Upto 3 sets allowed)

Type of Sensor: web / webgateway / mailgateway / browser Sensor Name Sensor IPAddress Date First Seen

Add Another Sensor

TakeDown Info (Upto 3 sets allowed)	Date: Agency Comments: Add Another TakeDown Info
Archive Site and Info (Up to 3 sets allowed)	Type of Archive: collectionsite / basecamp / sendercamp URL: Comments Add More Archive Data
Links to Other Data Related to this Incident (Upto 3 sets allowed)	URL: Add Another Related Info
Correlation Information (Upto 3 sets allowed)	Data: Add Correlatable Data

Enter any Additional Comments:

Click Here to Save to file named: phish.xml

XML makes reports human readable and assists in editing reports, adding data and organizing human-driven workflows

IODEF Extensions RFC at the Moment

- APWG working within the IETF to make this XML schema an IETF standard for ecrime reporting
  - Base specification for IODEF passed last month
  - APWG refiling its RFC for the IODEF-extensions
    - – Committee been reviewing proposal since June 2005
      - » Well received to date
  - – Expected to leave committee and be adopted by this Summer
- Asian, European and Australian companies, trade associations and CERTs (some already using IODEF) are already looking into adopting it for ecrime event reportage

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

If You’ve an Interest

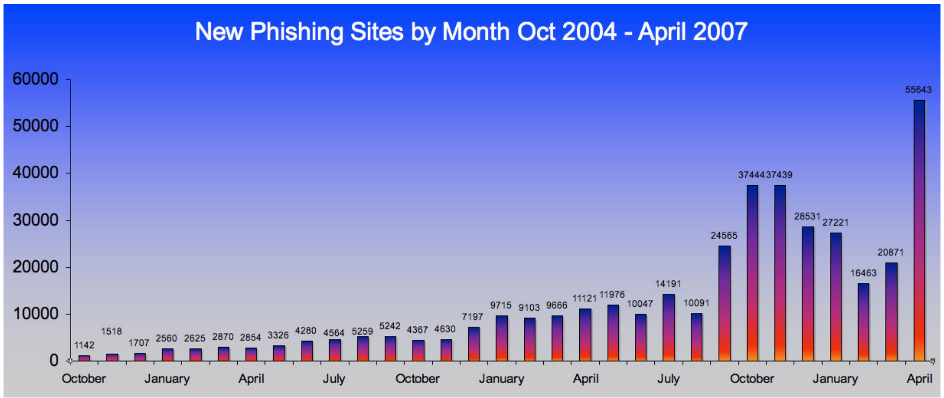
- Pat Cain, IETF committeeman and APWG Senior Research Fellow
  - pcain@antiphishing.org
- http://www.coopercain.com/incidents/index.htm

APWG eCrime Repository

APWG eCrime Data Repository & Block List

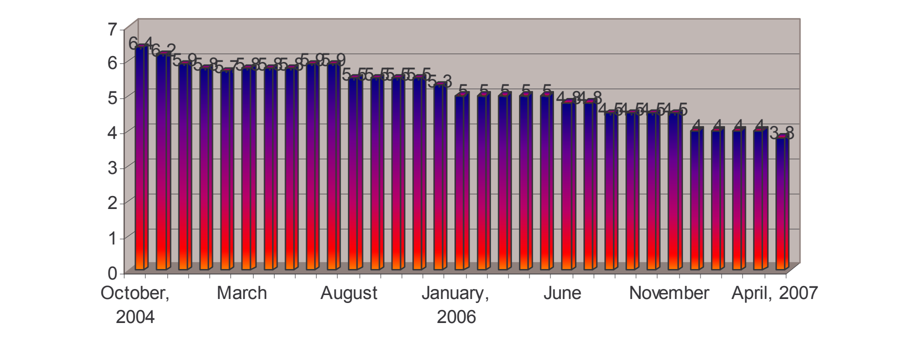
- **Collecting phishing data since October 2003**
  - 2,500,000-plus records archived thus far
    - 13,500-plus unique URLs added every month
- **Currently two principal Repository resources**
  - Historical archive
  - Block list updated every 5 minutes
  - Contains URLs from previous three days' reports
  - Generally, about a 10 megabyte file
  - Each URL has a 'confidence level' of certainty of its inauthenticity
  - Multiple uses in counter-ecrime technologies and forensics
    - Integrated browser anti-phishing systems
    - Standalone toolbars
    - Industrial research and development
    - University research
    - eCrime forensic analyses

Reporting & Blocking Makes More Work for Phishers


New Phishing Sites by Month Oct 2004 - April 2007

In this same period time-live for phishing sites has dropped to just four days

Time-Live for Phish Servers Drops to Under 4 Days



Time-live dropped steadily even as numbers of servers grew by large increments

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

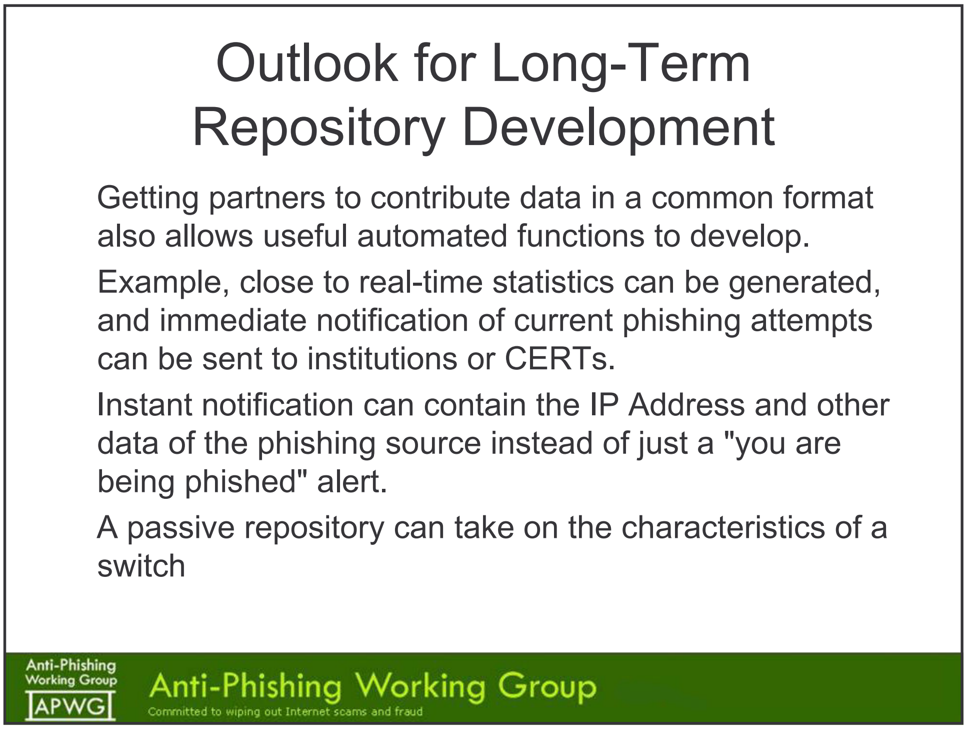
Repository & Block List Sources and Methods

- 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
  - Brandholders send confirmed URLs directly to the Repository
  - APWG member security and take-down companies send confirmed URLs directly to the Repository
  - Reportphishing@antiphishing.org send unconfirmed reports to APWG for processing
    - – Automated parsing pulls out relevant data and places it in Repository
  - Volunteer antiphishing organizations (PIRT and PhishTank)
  - Research partners
- Lots of room for expansion
  - – Some of the largest sources not yet exploited
    - Though we're talking with many of them now
  - – New contributing companies, groups and associations coming online regularly
- 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

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud



Outlook for Long-Term Repository Development

Getting partners to contribute data in a common format also allows useful automated functions to develop.

Example, close to real-time statistics can be generated, and immediate notification of current phishing attempts can be sent to institutions or CERTs.

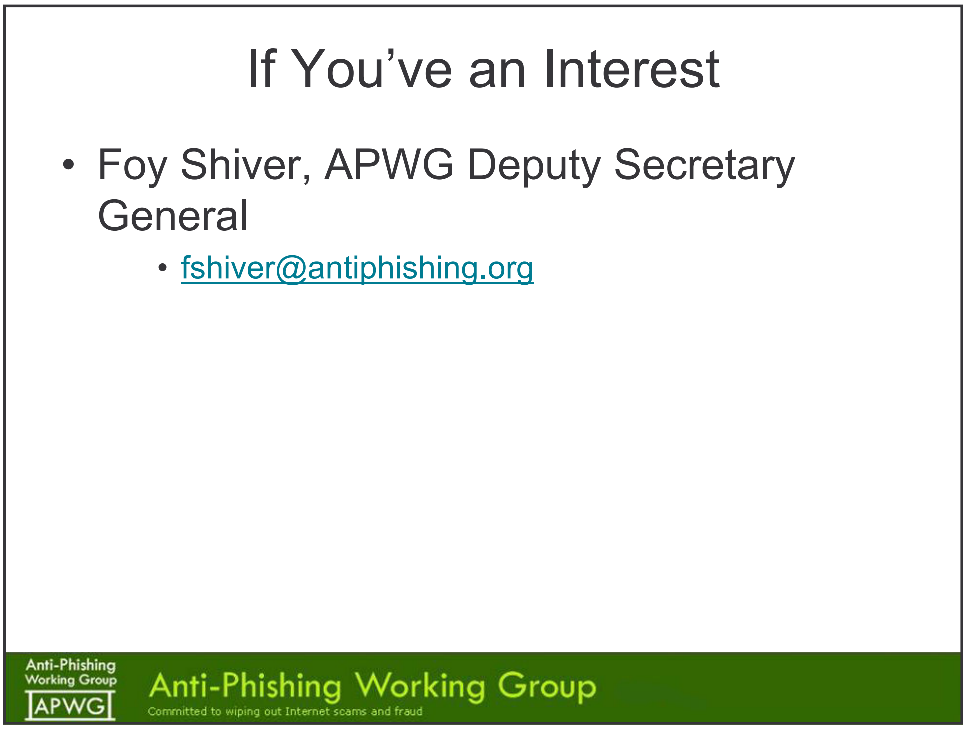
Instant notification can contain the IP Address and other data of the phishing source instead of just a "you are being phished" alert.

A passive repository can take on the characteristics of a switch

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud



If You've an Interest

- Foy Shiver, APWG Deputy Secretary General
  - fshiver@antiphishing.org

Anti-Phishing Working Group APWG

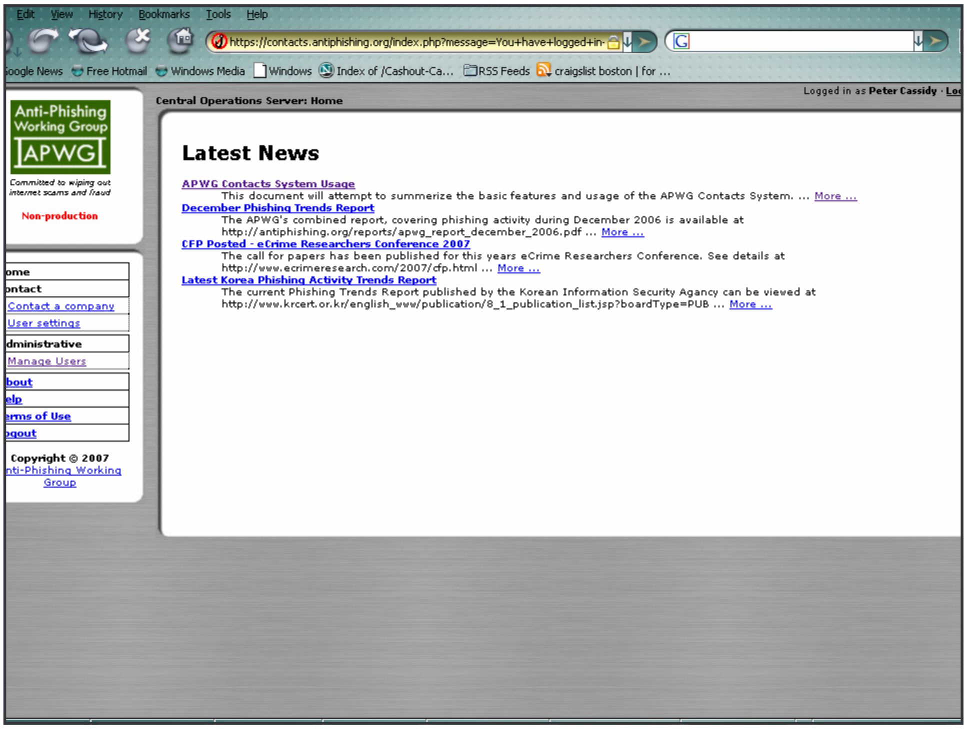
Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

APWG Contact System for Abuse Managers

APWG Contact System for Abuse Managers

- **APWG Contact System for Abuse Managers** allows companies who need to communicate about a phishing attack (typically ISPs and victimized brandholders) to find each other without exposing a large database
  - In Beta mode currently with some 1600 companies, CERTs, and government agencies' representatives enrolled
    - Cleaning up enrollments now and will be moving membership to locate and enroll proper forwarding address or specific personnel to have listed for contact
  - Organizing a standard User Agreement (Click through) for the Contacts system
    - User authorization to act on notices
    - Reasonable good faith effort
    - Refrain from using system for any other communications
  - Established new APWG membership level with single benefit: enrollment in the contacts system


Edit View History Bookmarks Tools Help
https://contacts.antiphishing.org/index.php?message=You+have+logged+in-
oogle News
Free Hotmail
Windows Media
Windows
Index of /Cashout-Ca...
RSS Feeds
craigslist boston | for ...
Anti-Phishing Working Group
APWG
Committed to wiping out internet scams and fraud
Non-production
ome
ontact
Contact a company
User settings
dministrative
Manage Users
bout
elp
erms of Use
ogout
Copyright © 2007
nti-Phishing Working Group

Logged in as **Peter Cassidy** · Lo

Central Operations Server: Home

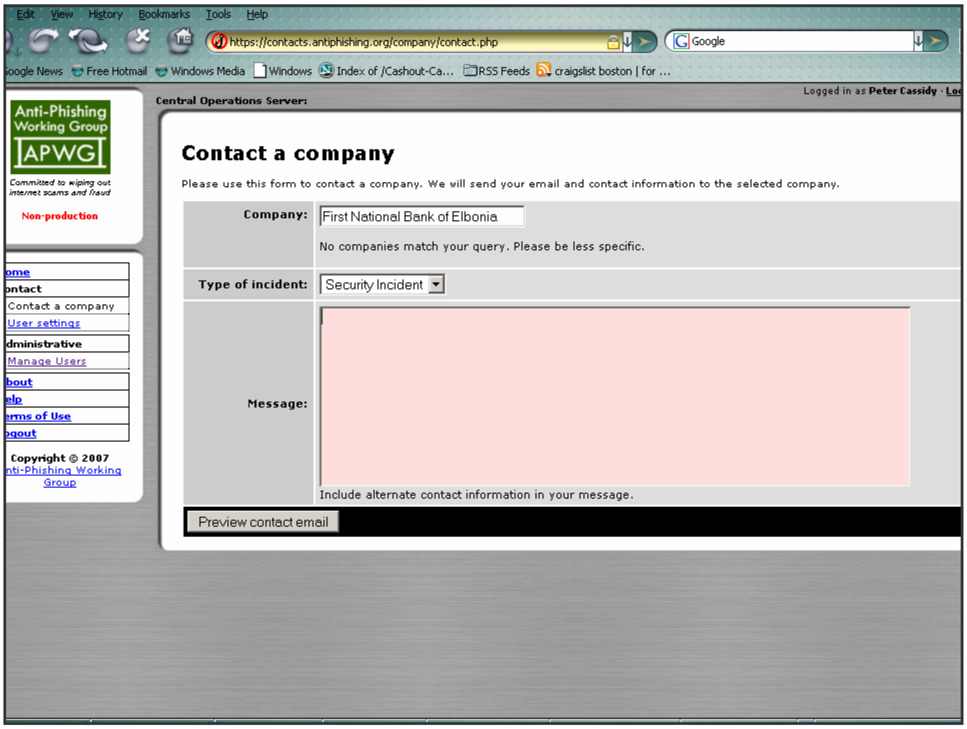
Latest News

APWG Contacts System Usage
This document will attempt to summerize the basic features and usage of the APWG Contacts System. ... More ...

December Phishing Trends Report
The APWG's combined report, covering phishing activity during December 2006 is available at http://antiphishing.org/reports/apwg_report_december_2006.pdf ... More ...

CFP Posted - eCrime Researchers Conference 2007
The call for papers has been published for this years eCrime Researchers Conference. See details at http://www.ecrimeresearch.com/2007/cfp.html ... More ...

Latest Korea Phishing Activity Trends Report
The current Phishing Trends Report published by the Korean Information Security Agancy can be viewed at http://www.krcert.or.kr/english_www/publication/8_1_publication_list.jsp?boardType=PUB ... More ...



Logged in as **Peter Cassidy** · Lo

Central Operations Server:

Contact a company

Please use this form to contact a company. We will send your email and contact information to the selected company.

Company: First National Bank of Elbonia
No companies match your query. Please be less specific.

Type of incident: Security Incident

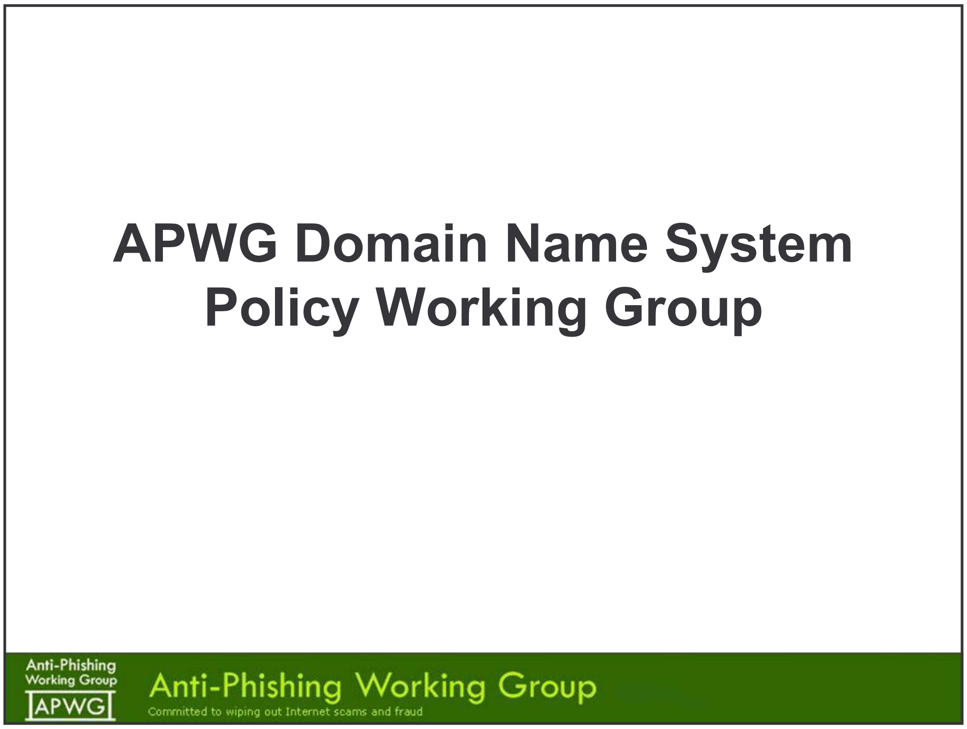
Message:
Include alternate contact information in your message.

APWG Contact System for Abuse Managers

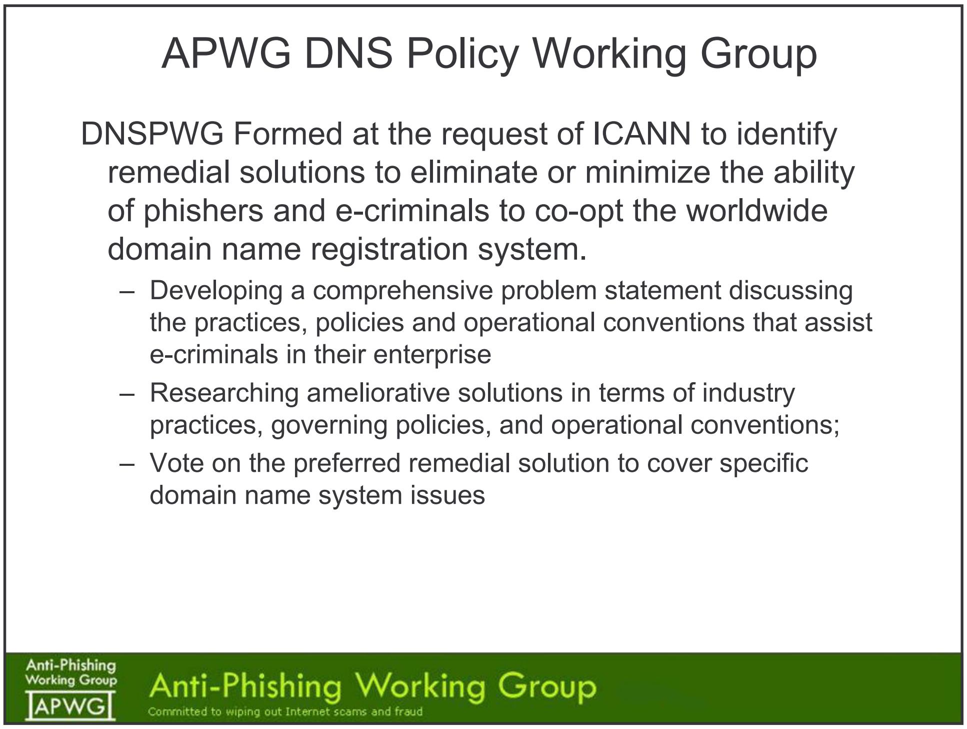
- – Discussions of federation of Abuse Manager Contact Systems under way with trade groups and response organizations
- – Throttled system (5 a day maximum) with reportage to administrators for users hitting maximum allotments
  - Working on scheme to discipline abusers of system, if they should arise
    - – Necessary part to organize robust federating agreements

If You’ve an Interest

- Foy Shiver, APWG Deputy Secretary General
  - fshiver@antiphishing.org



APWG Domain Name System Policy Working Group



APWG DNS Policy Working Group

DNSPWG Formed at the request of ICANN to identify remedial solutions to eliminate or minimize the ability of phishers and e-criminals to co-opt the worldwide domain name registration system.

- Developing a comprehensive problem statement discussing the practices, policies and operational conventions that assist e-criminals in their enterprise
- Researching ameliorative solutions in terms of industry practices, governing policies, and operational conventions;
- Vote on the preferred remedial solution to cover specific domain name system issues

Providing Research on WHOIS Proposals at the ICANN

- Operational Point of Contact (OPoC)
  - Provides for third-party cache of WHOIS data
- Special Circumstances Proposal
  - Keeps WHOIS data public but allows redaction of data for safety and other “special circumstances”
- APWG Role largely reportorial, providing ICANN with operational insight on how DNS and WHOIS data are exploited
  - Developing ICANN’s appreication of the role of the DNS in different kinds of Internet-mediated crime
- ALSO: Examining and developing .ASIA proposal for certifying third-party interveners who can ask registrars directly for expedited (an hour) removal of a domain name record

If You’ve an Interest

Foy Shiver, APWG Deputy Secretary General

fshiver@antiphishing.org

Or

Peter Cassidy, APWG Secretary General

pcassidy@antiphishing.org

Thank You

pcassidy@antiphishing.org

+1 617 669 1123