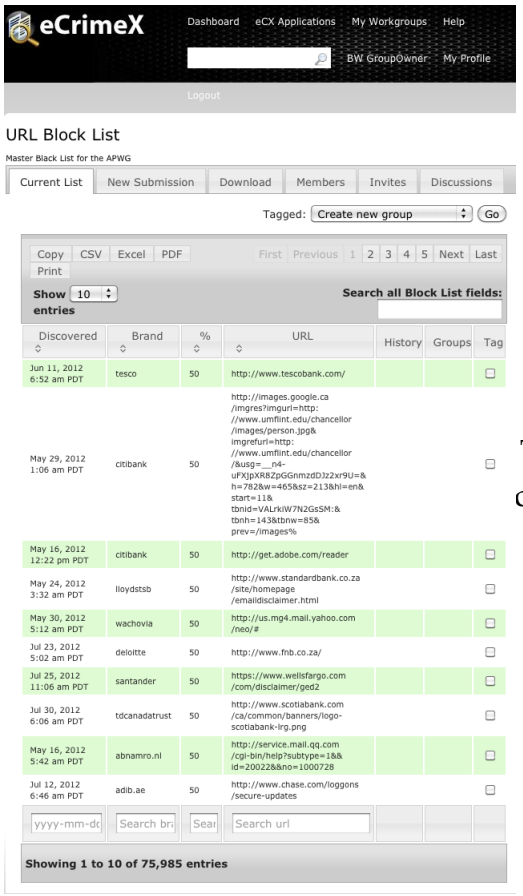
Accredited Reporter Program Introduction

APWG established its **URL Block List (UBL)** repository in 2003 under demand from industry and NGOs for a central clearinghouse to receive phishing reports from brand holders and responders, and to distribute them to developers of security software, such as browser security toolbars and anti-virus systems as well as to cybercrime investigators requiring notification of attacks. Since then responders and investigators from industry, government and NGO sectors have been motivated to route phishing reports in real time to the APWG's UBL to inform security applications and forensic programs, including:

- Rapid distribution of block lists for spam filters, browsers, anti-phishing toolbars, web filters and proxies
- Global protection of consumers and business from frauds involving commercial enterprises and brand-holders
- Prevention of users globally from downloading malicious software
- Prevention of users globally from disclosing login and password credentials
- Benchmarking efficacy against others in similar industries to determine if fraudsters are targeting them more intensely
- Creation of forensic databases for researchers, industrial investigators and law enforcement to better succeed in legal investigations and actions against criminals who multiple companies in common
- Data exchange with other members of the economy or government who are being affected by the same threats (phishing kits, malware distribution sites, botnet C&Cs, malicious IP addresses, reshippers, mules)

Any brandholder or responder that has cybercrime event data they want to be cleared through the UBL to alert software developers or inform investigators forensic toolsets, should be participating in the Accredited Reporter program which is described herein. An application form can be found on page 6.

Figure 1 UBL application on eCX



As the user base of the UBL expands, new applications for the data are continually suggested and considered for development under the APWG members' eCrime Exchange (eCX). Today, the APWG UBL is a dynamically updated archive of URLs and associated data that is submitted by the general public, APWG members, CERTs, cybercrime responders, contributing brand holders and data exchange correspondents. The UBL is housed on the eCX which currently eCX supports four different access points into the UBL data: Web-based application; internal eCX downloads; external downloads; and the UBL API.

The **APWG Accredited Reporter Data Submission Program** helps to broaden the number of qualified contributors to the UBL across the globe in order to maximize the trans-industrial exchange of event data related to cybercrime attacks. The program accomplishes this by establishing a formal mechanism for an enterprise to be accredited by the APWG **to send reports to the UBL directly** and, further, **to assign those reports a confidence factor commensurate with the expertise and authority of the reporter**. Higher confidence factors, of course, redound to greater trust and broader utility for those reports to be used for different kinds of security and forensic applications.

Qualifying organizations will be able to use their credentials to submit reports in bulk for processing, speeding the time of delivery to the UBL as well as accelerating processing and clearance of reports through the UBL to end users.

The formal submission of hand-processed and confirmed phish mails will allow reporters to mark their records with a confidence factor of 100%, giving these reporters broader utility to UBL users who induct the data feed into their security applications and forensic routines.

Application and Enrollment Requirements

The **Accredited Reporter Data Submission Program** is open to brand holders, national or industrial Computer Emergency Response Teams (or CSIRTs, IRTs, CIRTs or CSIRTs), security services companies, telecommunications companies or technology companies that regularly monitor phishing attacks (using either social engineering schemes or crimeware/technical subterfuge schemes) and/or malevolent electronic messaging.

Enrollment requires a formal application (See instructions and application form on page 6) to be completed and submitted to the APWG for review. Current APWG members are encouraged to inquire about their company's primary point of contact (Company Administrator) and to coordinate the application with their organization's APWG POC.

Data provided in program applications will be vetted by APWG and, if deemed eligible, the applicant will be contacted by the APWG and begin the process of enrolling them and their employer as an Accredited Reporter. (A program fee of $1000 is required for each application – renewable annually - though this requirement is waived for current members of the APWG as well as for all government agencies and non-profit institutions.) Upon receipt of the application, APWG will provide the applicant with an invoice and payment advice before beginning processing of the application.

Data Delivery and Formatting Requirements

The Accredited Reporter applicant that is accepted into the reporting system will be provided delivery mechanism or mechanisms appropriate to volume of reports expected to be submitted and level of data detail the reporter will be able to routinely provide.

Currently, large volume APWG contributing phishing reporters use a managed email delivery mechanism. As the program evolves, however, APWG will be establishing web-formed submission for low-volume submitters and an API set to enable a submission channel for the highest-volume reporters.

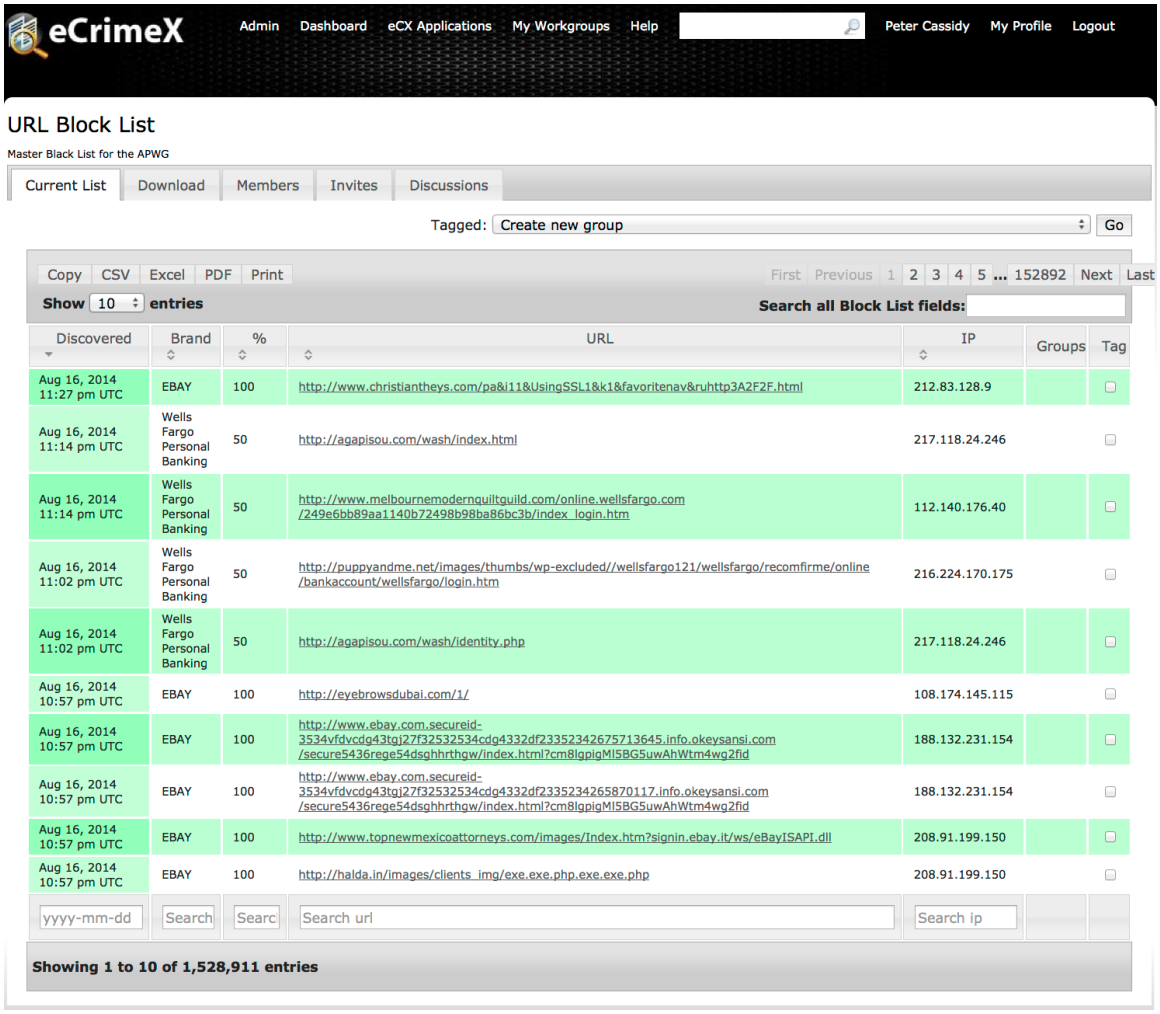


Figure 2
UBL table
on eCX

The Accredited Reporter will be expected to deliver reports of communications via Internet media that satisfy the contemporary definition of a phishing campaign, in order to limit the numbers of irrelevant records (e.g. gray-market spam, generic spyware) that the UBL would have to process, parse and discard. The most authoritative definitions today can be found at the APWG's eCrimeopedia at ecrimeopedia.apwg.org in which phish and phishing are, respectively, defined as:

> Phish - A criminal web site that attempts to steal user credentials by claiming to be the legitimate service.
>
> Phishing - The practice of sending false e-mails or instant messaging that typically look like they came from a legitimate business, requesting private or financial information, often via a click-through to another website a

fraudster has set up to look legitimate, but which is actually harvesting information. It tends to apply social engineering to pose as a trusted source.

APWG's URL Block List was established using a simple CSV format for record data elements.

Reporter Accreditation Maintenance

The accreditation of reporters will be reviewed on an ongoing basis and renewed on an annual basis. Measurement of reporting efficacy considered in renewal will be based on the numbers of false positives contributed by the reporter and confirmed as erroneous and removed from the UBL by the APWG.

In these renewal cycles, Accredited Reporters will be assessed according to the quality of their contributions to the UBL, measured as a proportion of records accepted into the database from the total contribution by the Accredited Reporter. Further, APWG reserves the right to revoke the reporter's accreditation and access to the UBL resources if its proportion of false positives consistently spikes beyond an unreasonable proportion of total contributed reports.

Instructions for Accredited Reporter Application

Interested parties need to complete, sign and date the application form on page 6, scan it and email it to reporter@apwg.org.

Accredited Reporter Application Form

_____
Applicant Name

_____
Company Name

_____
Business Type (Corporation, LLC, LTD, etc.)

_____
TaxID Number

_____
Primary Business Address
Street, City, State/Province, Country, Postal Code

_____
Primary Web Addresses

(_____) _____ (_____) _____
Primary Business Phone Applicant Business Phone

_____
Applicant Business Email Address

_____
Email Address to be used to forward reports

_____
Current APWG Member Yes___ No___

_____
APWG Member Referee

_____
Applicant Signature