Anti-Phishing Working Group

www.antiphishing.org

DNS Policy Sub-Committee Overview

Rod Rasmussen
Rod.Rasmussen@InternetIdentity.com

Anti-Phishing Working Group

- Launched in 2003
- 2600+ members
  - 1600+ companies and agencies (worldwide)
  - e-Commerce, financial, telecomm, ISP's, solution vendors, law enforcement, academics, national CERTs, etc.

- Focus: Eliminating fraud and identity theft that result from phishing, pharming and email spoofing of all types

APWG Successes

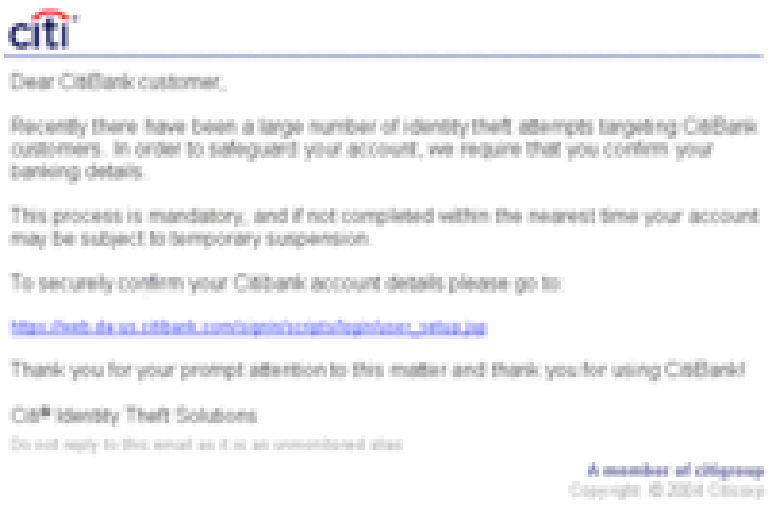
- Public Awareness and Education
- Phish Site URL Repository
  - Up several years; Everybody loves the statistics ☺
  - Submit URLs and a confidence factor to APWG
    - Every 5 minutes a new list of URLS to block is generated
    - Most big ISPs/Tools pull list to use in filters/blocking
    - Now includes DOMAIN NAMES registered for fraud
- Blind Contact List
  - Find a phished brand-owner via federated list
  - Submit to providers with fraud or hacking problem

DNS Policy Sub-Committee

- 39 members
- Participants include registries, CERT's, solution providers, ISP's, researchers, financial institutions, etc.
- Goal: Ensure that anti-phishing concerns are represented during the creation or modification of Domain Name System policies

Phishing Definition

Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and/or financial account credentials.


citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

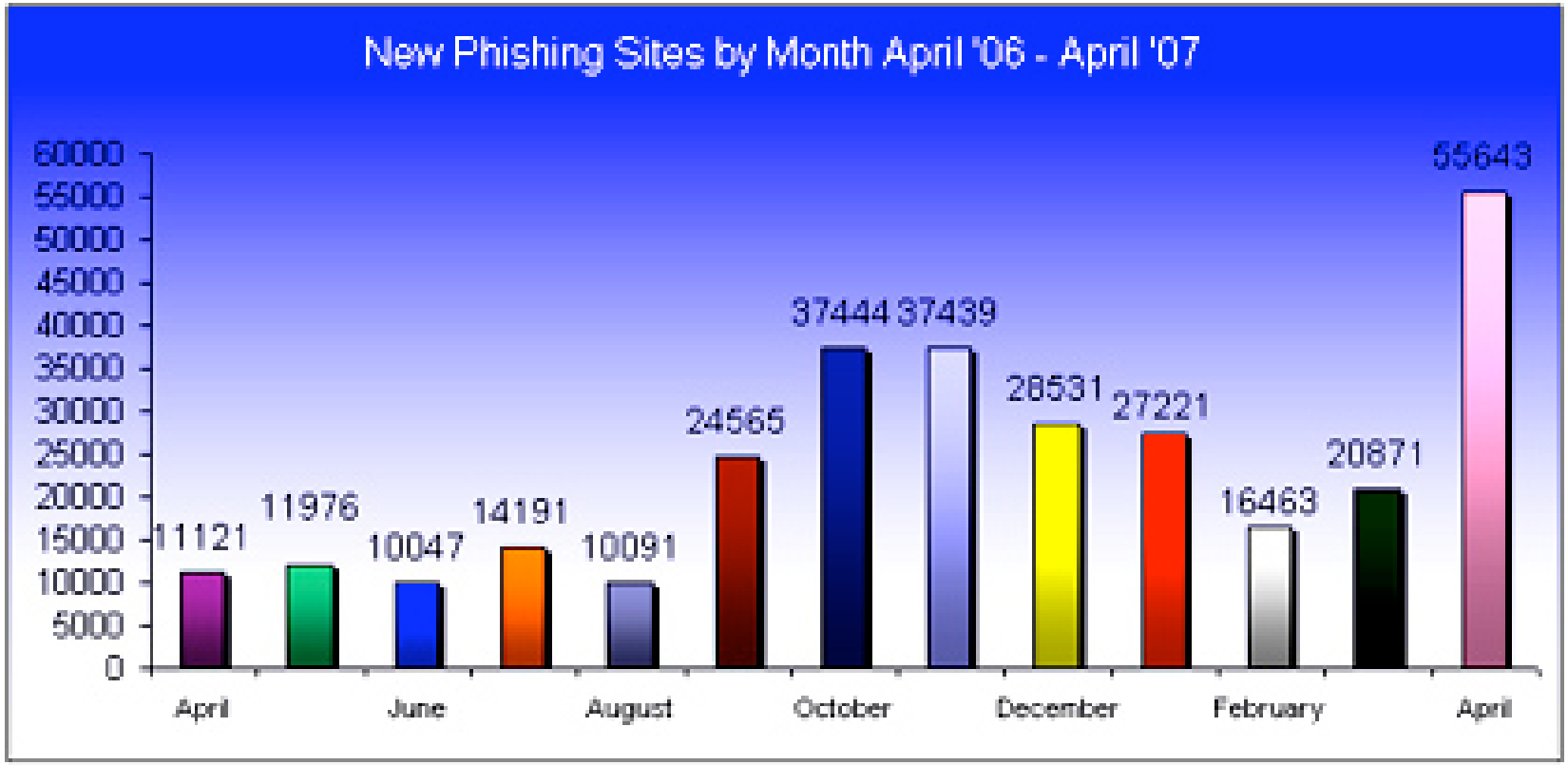
Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

The Overall Phishing System

- Lure to Potential Victims
  - Mainly email, but VOIP, IM, phone, letter are used
  - Malware (keystroke logger, worm) attached, too
- Web Interface to User/Victim
  - 'Personal' web pages, hacked servers, phish domains
  - Multiple DNS Servers, fast flux, all the good network engineering practices
- Collection Point
  - Server of some type, sometimes via e-mail drop-box
- Database

Number of Phishing Sites is Growing



Huge growth is due:

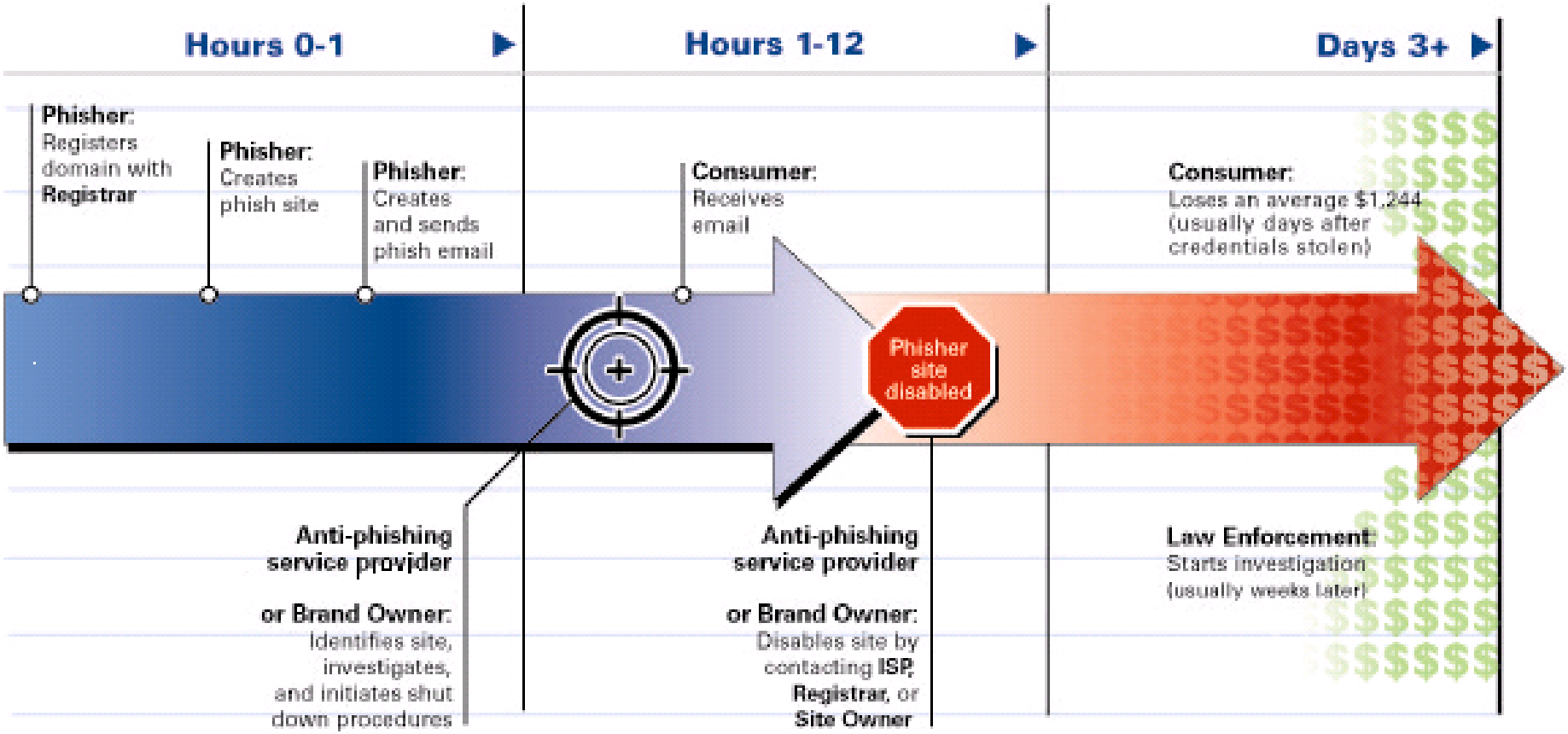
- The success of browser blocking in IE and Firefox
- RockPhish

Phishing is a Global Problem

Top countries for hosting phish sites in April 2007

Most Phish Sites Disabled within Hours

Usually NOT by law enforcement



Impact of the Problem

- Organized International Criminal Activity
- $182 million **reported** losses in 2005 (FBI IC3)
- $105 billion estimated cybercrime impact in 2004 (US Treasury Department)

APWG & ICANN Interaction To Date

- Several individuals members of both communities

- December 2005 Vancouver ICANN Meeting
  - Registrar Constituency Meeting - Briefing on Phishing
    - Best Practices from GoDaddy and NetSol
    - Info on phishing from Spamhaus, Internet Identity
    - Microsoft briefing on E-mail authentication

- November 2006 - APWG Meeting Orlando
  - Special session on domains used in phishing
    - ICANN represented by John Crain
    - GoDaddy, NetSol, Verisign also panelists
  - Constructive discussion with several ideas exchanged
  - Kicked-off formation of the APWG special subcommittee
    - DNSPWG to give recommendations to ICANN and registration community in 2007 per request by panelists

Initiatives of the DNS Policy Sub-Committee

- Participate in ICANN WHOIS Working Group
- Work with .asia on a registry phish domain suspension policy and registry best practices
- Work with registrars on phishing best practices

WHOIS Working Group Participation

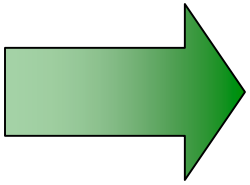
- Goal: Accommodate privacy concerns while maintaining phish site takedown efficacy

- WHOIS use cases for anti-phishing*:
  - Email, call, and fax the owner of a hacked site to help get his/her site cleaned up
  - Identify additional phish domains related to a phish domain (e.g., paypallogin.com, bofalogin.com, rbslogin.com)

(*) – White paper of WHOIS use cases is in your registration packet and available at
http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf

Main Points for ICANN WHOIS WG

- Most phish sites are taken down by brand owners or third party vendors, NOT law enforcement
- Phish site shutdown happens within hours
- Phish site shutdown often involves investigation via WHOIS data



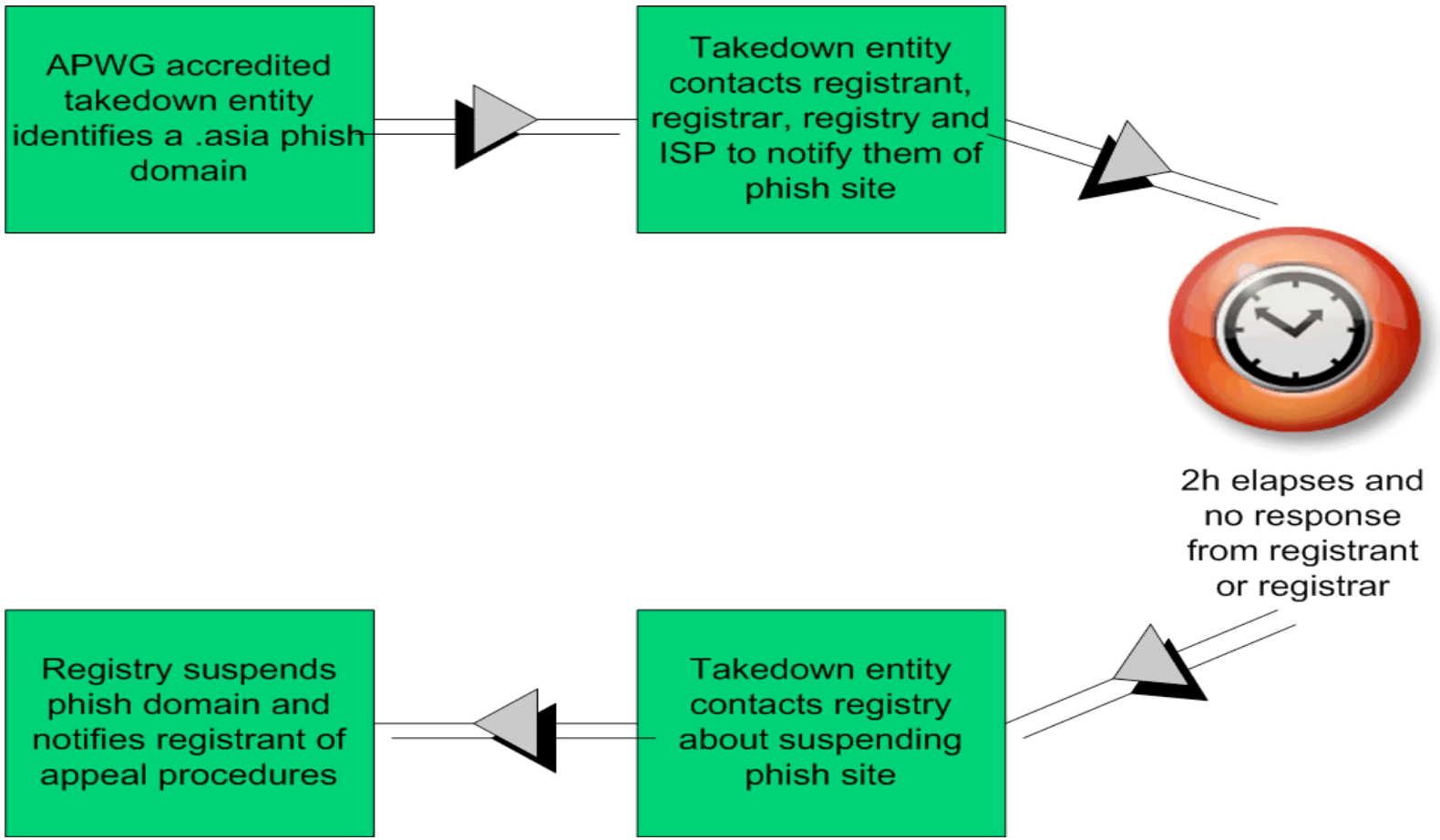
Protecting consumers from phishing requires brand owner and third party vendor real-time access to WHOIS data

Question: Can we find a way to allow this access while maintaining privacy for natural persons?

Initiatives of the DNS Policy Sub-Committee

- Participate in ICANN WHOIS Working Group
- Work with .asia on a registry phish domain suspension policy and registry best practices
- Work with registrars on phishing best practices

.asia Domain Suspension Initiative



Key Points of .asia Suspension Initiative

- APWG will create a committee that will define policy for takedown and accredit takedown entities
- Eliminates the problem of phish sites that are taken down and immediately come up again on a new ISP
- Create whitelist of sites (like Geocities) that could never get suspended
- Issues to be resolved
  - DNS caching
  - Appeal process
  - Determining sites that are whitelist eligible

Initiatives of the DNS Policy Sub-Committee

- Participate in ICANN WHOIS Working Group
- Work with .asia on a registry phish domain suspension policy and registry best practices
- Work with registrars on phishing best practices

Registrar Best Practices

- Goal: Provide **recommendations** to registrars to help them assist the anti-phishing community and make the Internet safer for all of us
- Focus:
  - Evidence preservation (help LE catch the criminals)
    - What is useful? How to preserve? Who to provide to?
  - Registration screening tips to identify fraudsters proactively
  - Phishing domain takedown assistance

Registrar Best Practices (cont)

- Understand the operational realities of the registrar business
- Can help registrars REDUCE costs:
  - Reduce fraudulent domain purchases/chargebacks
  - Reduce load on abuse departments
  - Limit potential legal liability
- Provide resources to help identify malicious activity

Summary

- These are works in progress – we are always looking for additional input
- If you would like to participate, please contact
  - Laura Mather, lmather@markmonitor.com
  - Rod Rasmussen, rod.rasmussen@internetidentity.com
  - Brad Keller, brad.keller@wachovia.com