Spam, Phishing & Trojans

CSH6 Chapter 20

"Spam, Phishing & Trojans: Attacks Meant to Fool"

Stephen Cobb

1

Topics

CSH6 Chapter 20

- Introduction
- Email Basics
- Spam (not SPAM™)
- Fighting Spam
- Phishing
- Trojan Code

Supplementary material added in June 2018 to update older statistics

2

Introduction

- Definitions
  - Spam = unsolicited commercial email
  - Phishing = use of deceptive spam to trick victims into clicking on dangerous links
  - Spear-phishing = use of targeted email to obtain confidential personal information
  - Trojan code = programs that have covert unauthorized functions (usually malicious)
- Serious consequences
  - Degradation in trustworthiness of email
  - High volume of spam uses bandwidth
  - Email has become vector for technological & social harm

3

Common Elements

- All use deception
  - Prey on gullibility
  - Some exploit greed
  - All depend on ignorance
- Enabled by system services
- Run at the application layer
- Often combined for additional power & harm
- Consistently underestimated at time of emergence – warnings met with skepticism & hostility
- Rapid proliferation
- Enormous social & technological costs
- Associated with growth of financial gain as prime motivator for malware & Internet abuse
- Some spammers trick companies into thinking they are sending legitimate publicity

4

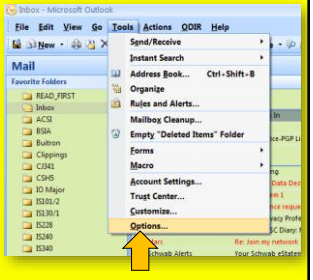
Email Basics

- Email at core of delivery method
  - SMTP – Simple Mail Transport Protocol
  - No process for verifying validity of FROM and TO data
- Attempts to add security to email transmission
  - Whitelist: allowable senders
    - ✓Difficult to maintain
    - ✓Slows processing significantly
  - Blacklist: forbidden senders
    - ✓Often wrong
    - ✓Can be fooled by bad actors into adding legitimate sites (e.g., University email being auto-forwarded to external email system)

5

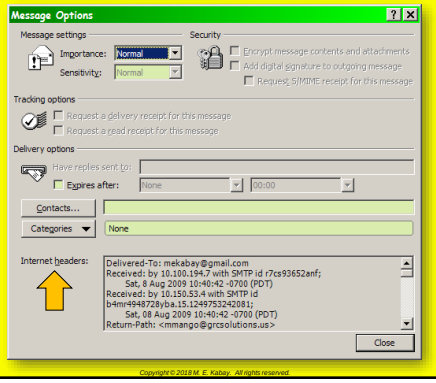
Email Headers (1)

- Every step in multistage transmission of email adds information to the *header*
- Email programs usually
  - Suppress header but
  - Allow user to examine header on demand
  - No guarantee of locating original sender



6

Email Headers (2)



Email Headers (3)

```
Delivered-To: mekabay@gmail.com
Received: by 10.100.194.7 with SMTP id r7cs31769anf;
        Fri, 7 Aug 2009 08:37:11 -0700 (PDT)
Received: by 10.210.59.5 with SMTP id h5mr1550646eba.48.1249659430313;
        Fri, 07 Aug 2009 08:37:10 -0700 (PDT)
Return-Path: <register@caloga.com>
Received: from xb73.caloga.com (xb73.caloga.com [195.154.149.73])
        by mx.google.com with ESMTP id
5si9030773ewy.76.2009.08.07.08.37.08;
        Fri, 07 Aug 2009 08:37:09 -0700 (PDT)
Received-SPF: pass (google.com: domain of register@caloga.com designates
195.154.149.73 as permitted sender) client-ip=195.154.149.73;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
register@caloga.com designates 195.154.149.73 as permitted sender)
smtp.mail=register@caloga.com; dkim=pass header.i=@caloga.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=caloga.com; s=b; h=To:Subject:From:Reply-To:Mime-Version:
        Content-Type:Message-Id:Date; bh=bJnEbQ995zW/silLnUF/1gdmA+VT9cP
        VDv3YTFIT6HM=; b=Nf5f1SEZsZymFZFJzqJE+LDcl2bENbAf0rs9yBwyuBaOVne
        epBUZJY2sVa505th4NdFkSkg2lt6YM5AhAvM+8VtowOt6htpvWkyyf8KXcDNzliB
        LAnEnBDEapmQxu+X/1JP2iHqHZdwrpygHWvNh0zdFh0TjvrQiQ4pQ3EdTdjc=
```

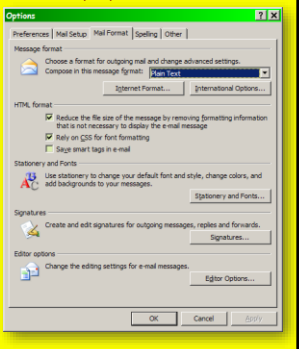

Email Headers (4)

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=simple; s=a; d=caloga.com;
        h=Received:To:Subject:From:Reply-To:Mime-Version:Content-
Type:Message-Id:Date;
        b=IchDBRKGQyNhQ4rUhJM6OXsRYZ7UlJkzYByQfPtzj7D8asqfE1kI/DjuAlPQOJ5
WuiR2c99CpmN2hSTRPCIlEsbRqDGZ9rVs5Y2ZjedCbblCMvevENZq2stmynTb0ISb;
Received: from www-data by caloga-deux.caloga.com with local (Exim 4.69)
        (envelope-from <register@caloga.com>)
        id 1MZRUd-0IAMxj-F9
        for mekabay@gmail.com; Fri, 07 Aug 2009 17:36:31 +0200
To: mekabay@gmail.com
Subject: Profitez de 30 euros offerts pour en gagner plus
From: PMU par Caloga <register@caloga.com>
Reply-To: PMU par Caloga <register@caloga.com>
Mime-Version: 1.0
Content-Type: multipart/alternative;
boundary="Part4a7bdac8ac973";charset="iso-8859-1"
Message-Id: <E1MZRUd-0IAMxj-F9>
Date: Fri, 07 Aug 2009 17:36:31 +0200
```

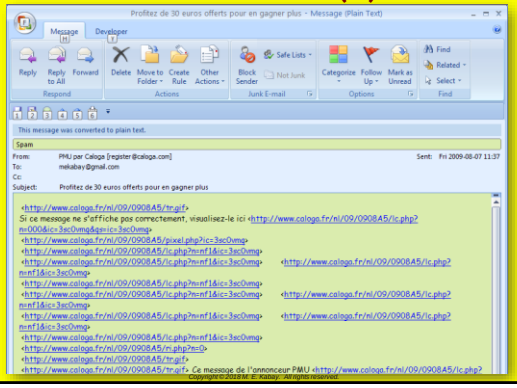
Visible in usual short header

Email Source Code (1)

- Early email systems transmitted plaintext messages
  - EBCDIC for IBM systems
  - ASCII for everything else
- HTML email
  - Supports formatting, stationery, visual signatures
  - Also supports malware, phishing



Email Source Code (2)



Spam Topics

- Origins & meaning of Spam (not SPAM™)
- Digging into Spam
- Spam's Two–Sided Threat
- Fighting Spam

Spam (not SPAM™)

- SPAM™ is a trademark of the Hormel Corporation for a canned meat product
  - Do NOT use SPAM in all uppercase to refer to unsolicited commercial email…
  - … except if entire text is uppercase, as in a title
  - May use "Spam" as first word in a sentence or "spam" elsewhere (Hormel does not object to these usages)
- Origin is the Monty Python skit about a restaurant where almost all the dishes have SPAM™ in them
  - http://pythonline.com/node/18297641
- Applied 1st to MUDs, then BBS, then USENET

13

Spam & the USENET

- USENET is early form of social networking
  - Vast array of special-interest discussion groups
  - Spammers ruined USENET as medium of exchange – barrage of repetitious, unwanted commercial messages
- Spammers harvested email addresses from USENET posts
  - Was the custom to include email address in postings
  - Custom declined after mid-1990s due to abuse by spammers
- Spam volume reached 85% of all email by 2005

14

Digging Into Spam

- Definitions
- Get Rich Quick
- Crime & Punishment
- Wasteful Game
- Magnitude of the Problem

15

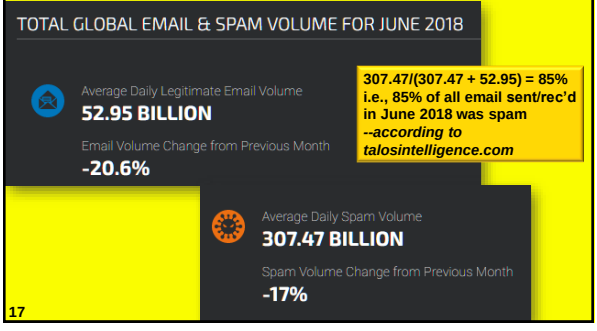
Defining Spam

- Unsolicited Commercial Email (UCE)
  - Early definition
  - Emphasized types of unwanted email that involved money
- Other forms of unsolicited email criticized or defended
  - Political messages
  - Announcements of noncommercial events (conferences, art shows….)
  - Charity requests
- Questions about meaning of "unsolicited"
  - Spammers use any excuse to weasel around definitions of *unsolicited*
- Even legitimate companies tempted to spam

16

Spam Statistics (1)

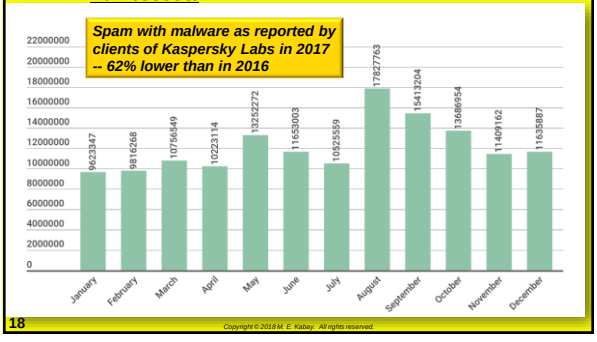
- https://www.talosintelligence.com/reputation_center/email_rep



17

Spam Statistics (2)

- https://securelist.com/spam-and-phishing-in-2017/83833/



18

Get Rich Quick (1)

- Spamming can be profitable
  - Costs low or zero (esp. for pirate users of open spam relays – SMTP servers without security and botnet herders)
  - Even tiny % of responses from suckers can generate significant profit through fraud/theft
- C. P. Direct (spammers in Arizona) shut down 2002
  - Sold $70M worthless anatomy-expanding pills
  - Refused to grant refunds when victims complained
  - Significant assets found by FBI
    - ✓$3M cash + jewelry
    - ✓Bank account balances totaled >$20M
    - ✓12 imported luxury cars (e.g., Lamborghini)
    - ✓Owned office building + luxury real estate

19

Get Rich Quick (2)

- Selling spam also source of profit for criminals
  - Approach naïve companies
  - Claim to have huge lists of highly tailored opt-in targets
  - Charge for spam sent indiscriminately to anyone on lists

- Victims typically businesses in developing world
  - Growing frequency of such cases from PRC
  - Exacerbated by language difficulties
  - Hardworking people are primary victims; recipients are secondary victims

20

Crime & Punishment

- Risk of prosecution and severity of punishment are minor
- *C. P. Direct* perpetrators
  - Michael Consoli & Vincent Passafiume pled guilty Aug 2003
  - Out of jail before May 2004
  - Petitioned Arizona Court of Appeals to overturn convictions and return their loot
- Jeremy Jaynes: a Top-Ten Spammer in 2003
  - Sent out 10M spam msg/day for $750K/mo profit
  - Convicted 2004, sentenced to 9 years prison
  - Appealed conviction on constitutional grounds (see next slide)

21

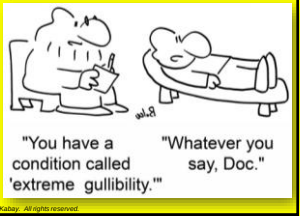
Jeremy Jaynes Absolved

- Basis from litigants for case before VA Court of Appeals (2006)
  - Claim: VA anti-spam law violates Commerce Clause by regulating email sent outside state
  - Claim: Violates First Amendment because spam is form of free speech
  - Court of Appeals rejected both arguments
- VA Supreme Court first round (Feb 2008)
  - Rejected standing to raise 1st amendment defense
- VA Supreme Court second round (Sep 2008)
  - Rehearing: *accepted* standing for 1st Amendment
  - *Reversed* its earlier ruling and *vacated* convictions on grounds that anti-spam statue did violate 1st Amendment by being overbroad (!)
- SCOTUS refused writ of *certiori* and declined to review case – ruling stands as a precedent

22

Spam a Wasteful Game (1)

- Play on gullibility
  - Send money to learn how to earn money easily
  - Sometimes response is to send spam teaching how to earn money by sending spam….
- Other widespread scams
  - Pump 'n' dump schemes (raise/lower value of stock through spammed lies)
  - Phishing schemes discussed later
  - Nigerian 419 fraud & fake lottery winnings (advance-fee fraud)



23

Wasteful Game (2)

Costs borne by

- Email recipients
  - Waste time sorting through spam to find good email
  - Pays to receive email (someone always pays for Internet connection)
- Enterprises
  - Lost productivity due to delay in finding real email
  - Costs of anti-spam measures
  - Wasted resources (bandwidth, disk space, CPU)

24

Wasteful Game (3)

- ISPs
  - Wasted resources (bandwidth, disk space, CPU)
  - Spam filtering costs, | administration
  - Policing users to prevent blacklisting
- Other economic factors
  - Depressed economy seems to increase gullibility & therefore spam
  - Spammers use as much bandwidth as they can get, so battle is never-ending

25

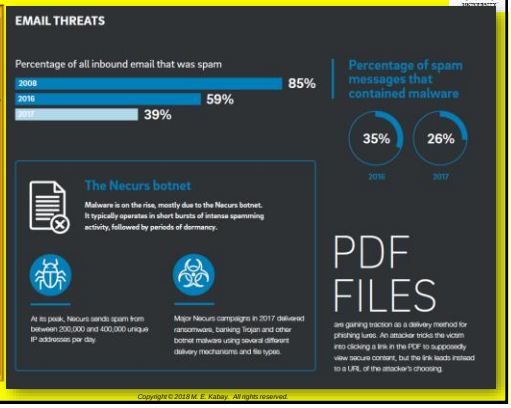
Magnitude of the Problem (1)

- Misperception that spam is not significant
  - Newbies
  - Office-only users whose email is filtered before they see it – thus little spam in their inbox
- Proportion of all email that is spam has grown rapidly
  - 1994 – 0%
  - 2002 – 50%
  - 2013 & later – 80-90% depending on source of statistics
- Major effects on ISP infrastructure
  - Disk storage
  - Bandwidth
- See graphs from Symantec on next 2 slides

26

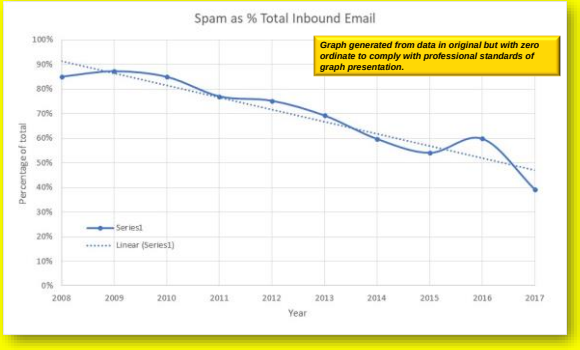
Magnitude of the Problem (2)

https://www2.trustwave.com/GlobalSecurityReport.html



27

Magnitude of the Problem (3)



https://www2.trustwave.com/GlobalSecurityReport.html

28

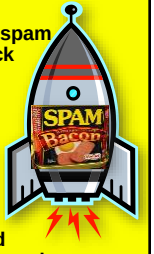
Spam's Two–Sided Threat

- Threat to resources well documented
  - As discussed in previous sections
  - Damages to a modest company can easily be counted in $M/year
- But other side is risk that employee will involve organization in sending spam
- Topics of following slides:
  - Threat of Outbound Spam
  - Mass E-Mail Precautions
  - Appending & Permission Issues

29

Threat of Outbound Spam

- Rogue marketeers can be tempted to spam for what they hope will be cheap, quick results
- Damage to organization
  - Damage relations with existing customers
  - Alienate potential customers
  - Tarnish reputation
  - All outbound email may be blocked once company associated with spamming
  - Retaliation (see next slide)



30

NETWORKWORLD (Dec 1994)

Anonymous executive – USETNET spam

- Posted advertising to 20 USENET news groups
  - Stupidly posted message 20 times instead of once to 20 groups – readers received *multiple copies* of spam
- Thought people would be interested
- Consequences
  - Email bombs sent to company email addresses
  - Toll-free number posted in *alt.sex* groups
    - ✓Thousands of obscene phone calls
    - ✓One receptionist quit in disgust
    - ✓Other sent all toll-free calls directly to his phone
  - Nearly destroyed his career
- Urged readers never to do such a stupid thing!

31

Mass E-Mail Precautions

- Never send email unless you are sure you know what it will look like to recipient
  - ❑Don't assume formatted email accepted
  - ❑Perhaps append a PDF formatted document
- Address field
  - ❑Use TO: only for few people directly involved
  - ❑Use CC: only for few people who may want to respond to each other
  - ❑OTHERWISE, use BCC to hide all the addressees
    - ✓Reduce wasted email from REPLY ALL
    - ✓Protect confidentiality of recipients
    - ✓Reduce access to addresses by spammers

32

Six Resolutions for Responsible E-Mailers

1. Don't falsify origin or use dummy IP address
2. Don't use misleading/false SUBJECT line
3. Include option in message for unsubscribing
4. Inform respondent of purpose of collecting email address
5. Don't harvest email addresses to spam people
6. Do not send bulk unsolicited email to people who do not have a *prior established business or personal relationship* to the sender

Council for Responsible E-Mail
Association for Interactive Marketing
Direct Market Association

33

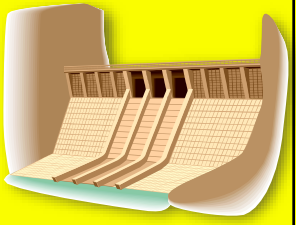
Appending & Permission Issues

- Companies called *email appenders* offer to find email addresses for customers who have not provided them
- Some of the email addresses are wrong: not right person – raises privacy issues
- Some recipients object to harvesting and use of their email address without permission
- May violate written privacy policy: legal liability

34

Fighting Spam

- Spam Fighters
- Good Reputation
- Relaying Trouble
- Black Holes & Block Lists
- Spam Filters
- Network Devices
- Email Authentication
- Industry Initiatives
- Legal Remedies



35

Spam Fighters: CAUCE

Coalition Against Unsolicited Commercial Email

- http://cauce.org
- CAUCE US founded 1997 by USENET members in news.admin.net-abuse.email & SPAM-L mailing list
- CAUCE North America joined CAUCE US & CAUCE Canada.
- Instrumental in passing antispam laws

36

Spam Fighters: Spamhaus (1)

Spamhaus Project founded 1998 by Steve Linford

- http://www.spamhaus.org
- Goals
  - Tracks the Internet's spammers, spam gangs & spam services
  - Provides dependable real-time anti-spam protection for Internet networks
  - Works with law enforcement to identify and pursue spammers worldwide
- (cont'd on next slide)

THE SPAMHAUS PROJECT

37

Spam Fighters: Spamhaus (2)

- SBL: Spamhaus Block List
  - http://www.spamhaus.org/sbl/index.lasso
  - Real-time database of IP addresses
    - ✓Verified spam sources & operations
    - ✓Free for email administrators
- XBL: Exploits Block List
  - http://www.spamhaus.org/xbl/index.lasso
  - Real-time database of IP addresses of hijacked PCs
  - Including open proxies, worms/viruses with spam engines…
- PBL: Policy Block List
  - http://www.spamhaus.org/pbl/index.lasso
  - Database of IP address ranges that should never deliver SMTP email to Internet mail server except their own
  - Maintained in collaboration from ISPs and network admins

SBL Advisory

XBL Advisory

PBL Advisory

38

Commercial Antispam Products

- Began in late 1990s as filters for individuals
- Some well-known appliances & services
  - Brightmail (Symantec) http://tinyurl.com/lcyl33
  - Postini (Google) http://tinyurl.com/r77p7v
  - IronPort (Cisco) http://www.ironport.com/
  - Cloudmark http://www.cloudmark.com/
  - SPAMfighter http://www.spamfighter.com/
- Open-source: Apache SpamAssassin Project
  - http://spamassassin.apache.org/

These references are not endorsements.

39

Whitelisting

- Respond to unknown senders
- Ask for human interaction
- Approve once forever
- Use CAPTCHA* to prevent automated response

40

Good Reputation

- Theory: recognize reliable/trustworthy sources
- Challenge-response
  - EarthLink ISP rolled out system in 2003
  - First time one sends email to EarthLink customer, must respond to query email before being allowed through
  - But some legitimate sources have no-response return addresses
- Whitelist
  - Maintain list of sources that are deemed reliable
- Cryptographic seal
  - Establish authentic origin
  - ePrivacy Group project failed to win sufficient market share to be effective
  - S/MIME digital signatures might also work

41

Relaying Trouble

- ISPs almost universally ban spamming
  - Exceptions are criminal organizations providing spam services
- Open spam relays
  - SMTP servers that do not require identification & authentication to send mail
  - Grounds for black-holing
  - Still some open relays left on the 'Net due to administrative laziness / irresponsibility
- Botnets *create their own SMTP servers* (daemons) on compromised computers

42

Black Holes & Block Lists

- Catalog IP addresses that have sent out significant volumes of spam
  - Direct originators
  - Open spam relays
  - Compromised by botnet daemons
- User systems check list before passing on email – or drop packets Original black hole list: MAPS RBL
  - Mail Abuse Prevention System Realtime Blackhole List (1997, Paul Vixie)
  - Sold to TREND Micro in 2005
  - Renamed *Email Reputation Services*
  - http://tinyurl.com/43q9dp
- Other products also include black holes (see earlier slides)

43

Spam Filters

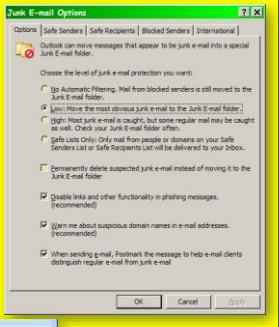
Content filtering another approach

- End-user Filters
- ISP Filtering
- Filtering Services
- Collateral Damage

44

End-user Filters

- Individual email client settings available
  - Can automatically file email from known correspondents into separate mailboxes
  - Rest can be examined more quickly
- Commercial products compile databases of signatures
  - Anything missed can be reported by user



45

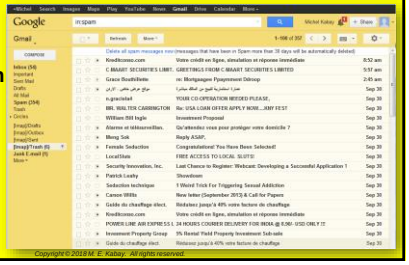
ISP Filtering (1)

- Concern about content-based filtering
  - Construed as privacy invasion
  - Risks of false-positives
- Formerly focused on SUBJECT field
  - Hence spammers use variant spellings & bizarre punctuation to avoid filters
- Public ISPs face legal issues
  - Status as equivalent of common carriers at risk if they filter too aggressively
- Individual corporations have no legal constraints
  - No privacy rights involved
  - No legal obligation to deliver unwanted email

46

ISP Filtering (2)

- Filtering getting better
  - Using user intervention ("not spam" & "is spam") to tighten filtering
  - Origination filters; e.g., block all .RU or .CN
  - Language filters; e.g., block all non-Western language sets



47

Filtering Services

- Redirect all client's email to their servers
- Use wide range of spam-spotting techniques
  - Block lists
  - Header analysis
  - Content analysis
  - Known-spam signature comparisons
  - Heuristic filtering for spam-like features
  - Whitelisting
- Enormous volumes allow refinements in filtering algorithms
- Collective intelligence schemes rely on users to vote on whether message is spam
  - E.g., Cloudmark
  - Reliability of voter determines weight (thus eliminating spammers' votes for their own spam)

48

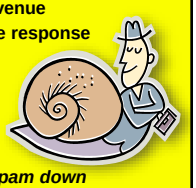
Collateral Damage

- Spammers can keep spamming
  - Costs of resources fall on the victims, not the spammers
  - Nothing prevents spammers from trying new methods
  - Overall resource utilization slows email, uses processing & other resources on many systems
- Type I & Type II errors
  - Type I error: false positive – mistakenly classifying legitimate email as spam
  - Type II error: false negative – failing to recognize spam

49

Network Devices

- One approach to attacking spammers is to track the money
- Most spam designed to generate revenue
  - Therefore always some legitimate response address
    - ✓Email
    - ✓Web site
- But Web addresses for spammers disappear / mutate rapidly
- Therefore key response is to *slow spam down*
  - Delay spam (or spam suspects) using antispam router and *traffic shaping*
  - Delay is disaster for spammer, negligible for legitimate traffic



50

Email Authentication

- If real sender of email were known, would greatly interfere with spammers' spoofing
  - Several attempts to add authentication of sender's domain name to email
- Sender Policy Framework (SFP)
  http://www.openspf.org/
- Certified Server Validation (CSV)
  http://mipassoc.org/csv/
- SenderID (Microsoft)
  http://tinyurl.com/9rs9b
- DomainKeys Identified Mail (DKIM)
  http://www.dkim.org/

51

Legal Remedies

- US CAN-SPAM Act of 2003
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act
  - Enforced by FTC
  - Bans false / misleading header info
  - Prohibits deceptive subject lines
  - Requires inclusion of opt-out method
  - Requires self-labeling as advertisement & valid physical postal address
- *Complete failure – no visible effect whatsoever*
- Led to Prof Kabay's all-time favorite *Network World Security Strategies* column title: "CAN CAN-SPAM CAN SPAM?"

52

Phishing

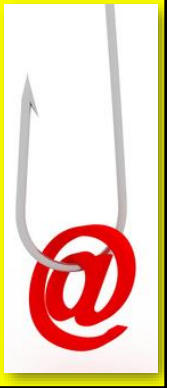
- Defining Phishing
- What Phish Look Like
- Growth & Extent of Phishing
- Where is the Threat?
- Phish Fighting

Image provided courtesy of
How Stuff Works.com
http://computer.howstuffworks.com

53

Defining Phishing

- Use of spam to fish for personally identifiable information (PII)
- Try to simulate official-looking email to fool victims into cooperating
- Aim is financial fraud
- Began ~2004
- Has grown steadily & become major problem
- Variants include *spear phishing*
  - Claiming that email comes from recognizable origin; e.g., HelpDesk at specific company
  - Targets employees in specific organization



54

What Phish Look Like (1)

- Simulate appearance of legitimate-looking email
  - Logos
  - Typefaces
  - Links *labeled* with credible URLs
- Glaring errors
  - Many phishing scams run by non-native English speakers
  - Full of spelling & grammar mistakes
- Logic errors that should be caught by recipients (but are often overlooked)
  - Why would anyone sign into a Web site to confirm a compromised userID/password combo? Doesn't make sense!

55

What Phish Look Like (2)

- Clues that a message is bogus
- Deceptive links – check source of email
  - Descriptions don't match underlying URLs
  - Numerical IP addresses conceal foreign sites
- Request to change PIN or password
  - As described in previous slide, does not make sense
  - No legitimate agency/bank would request such a thing
- Generic greetings (Dear Customer – or "Cutsomer")
- Bad spelling and grammar
- Masking specific details (e.g., no name of bank)

56

Examples of Attacks

- In examples shown in next slides, pay attention to details
- Look for
  - Bad spelling
  - Poor grammar
  - Logos
  - Bad links
  - Nonsensical offers
  - Illogical demands

57

People's Bank

Eh???

peoples.com

Dear People member.
We ask you to confirm immediately of your parity the account to given e-mail.

www.people-onlinebank.net

Otherwise we stop temporarily service of your account.
Thank you for using Suntrust Bank!

Please do not reaply this letter.
Again, thank you for using People.com

Not the proper domain for peoples.com

Duhhh ...

58

Citibank (Nov 10)

Dear Citibank Customer

We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking here.

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Links to http://82.90.165.65/citi

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

59

PayPal (1)

PayPal

Security Center

Military Grade Encryption is Only the Start

At PayPal, we want to increase your security and comfort level with every trans... Buyer and Seller Prote... Verification and Repu... keep you safe.

Why would we do this if our account is compromised?

We recently noticed one or more attempts to log in to your PayPal ... from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.

60

PayPal (2)

Actually links to http://212.45.13.185/.paypal/index.php

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend to verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,
PayPal Account Review Department
PayPal, an eBay Company

PayPal VERIFIED

61

Citibank (Nov 1, 2004)

Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced some new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

This security update will be effective immediately. Please sign on to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.

Citibank Online

Copyright © 2004 Citicorp

Links to http://200.189.70.90/citi/

62

eBay (1)

Dear eBay customer,

During our regularly scheduled account maintenance and verification proce

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an inte error within our processors.

Please update and verify your information by clicking the link below:

https://cgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo

If your account information is not updated within **48 hours** then your ability to sell or bid on eBay will become restricted.

http://signin-ebay.com-cgi-bin.tk/eBaydll.php which is in TOKELAU, South Pacific

63

eBay (2) – Detailed Analysis

Received by MK 2004-11-17

Welcome to eBay

Dear valued customer — Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

reviewed by TRUSTe site privacy statement

64

eBay(2) Source Code

Extract of relevant section:

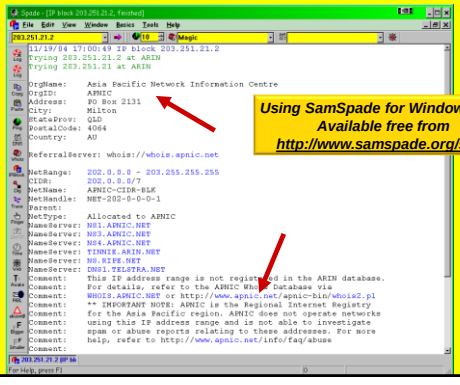
<p><STRONG><FONT face=arial>We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please </FONT><A

href="http://203.251.21.2/signin.ebay.com/ws2/eBayISAPI.dll/b2baf0b6a57d39abd6c44b48d6fe3559112c21e54b7e705ecc5116b3c7c38c37949e8aa81848934faf0821be04210e8c2ded3c4159edbee3ee1439f3892a3e91/"

**target=_blank><FONT face=arial color=#0000ff>click here</FONT></A></STRONG><FONT face=arial> and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.
**

65

eBay (2) Reverse IP Lookup



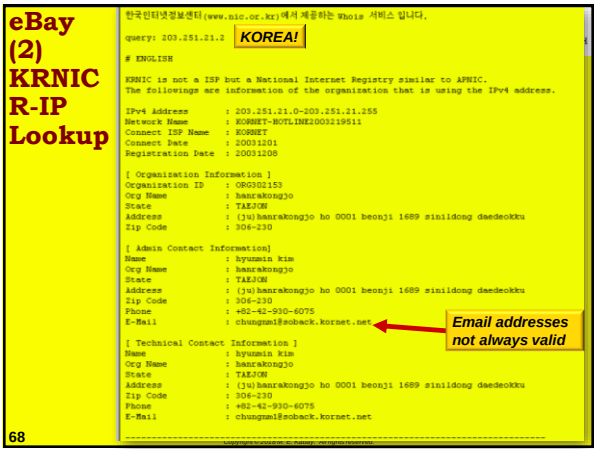
66

eBay (2) APNIC R-IP Lookup

Asia-Pacific Network Information Center Routes to KoreaNIC

67

eBay (2) KRNIC R-IP Lookup



68

Growth & Extent of Phishing

- Anti Phishing Working Group (APWG) documents phenomenon
  - http://apwg.org/
  - Extensive reports with graphs & analysis
- See extracts from most recent quarterly report on next slides: ***Phishing Activity Trends Report***

APWG Committed to Wiping Out Internet Scams and Fraud

69

Keyloggers & Redirectors

- Keyloggers record and upload your passwords (and everything else) typed on keyboard
- Redirectors send compromised users to dangerous Web pages
  - Can modify Domain Name System (DNS) servers to pass back wrong addresses
  - Or install local drivers on infected workstations to send traffic to fraudulent DNS servers
  - Or filter lookups for specific redirection to criminal sites

70

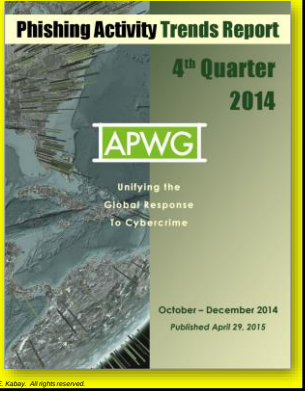
Where is the Threat?

- Individuals
  - Victimized by gullibility, ignorance
  - FTC & others trying to teach public wariness
  - Not working very well
- Companies & e-commerce
  - Too many people use same password / PIN on all their accounts
  - Compromise using phishing on personal info may open up corporate systems, national security assets
  - Undermine consumer trust in vendor

71

APWG Phishing Activity Trends (2014)

- Anti-Phishing Working Group (APWG)
  - http://apwg.org/
- APWG Phishing Attack Trends Reports
- Started 2004-01
- Valuable resources for term paper!



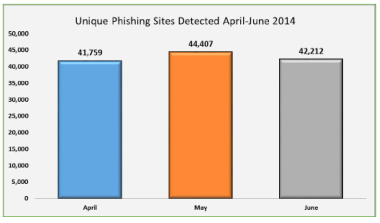
APWG Committed to Wiping Out Internet Scams and Fraud

https://apwg.org/resources/apwg-reports/

72

APWG Phishing Activity Trends (2014)

2014 Brand Attacks Aim at the Most Vulnerable Targets

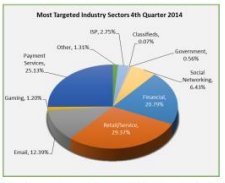


April through June 2014 saw the second-highest number of phishing sites ever observed in a quarter. [p. 4]

73

APWG Phishing Activity Trends (2014)

Retail/Service Was Most-Targeted Industry Sector in Q4



Retail/Service was the most-targeted industry sector in the fourth quarter of 2014, with Payment Services close behind. [pg. 7]

4th Quarter 2014 Phishing Activity Trends Summary

- During the 4th quarter of 2014, a record number of malware variants were detected – an average of 255,000 new threats each day. [p. 8]
- The number of unique phishing reports submitted to APWG during Q4 was 197,252. This was an increase of 18 percent from the 163,333 received in Q3 of 2014. [p. 4]
- The total number of phish observed in Q4 was 46,824. [p. 4]
- A total of 437 brands were targeted by phishers in Q4. [p. 6]
- The United States continued to be the top country hosting phishing sites. [p. 7]
- The United States remained the top country hosting phishing-based Trojans and downloaders during the three month period. [p. 10]

74

APWG Phishing Activity Trends (2014)

Statistical Highlights for 4th Quarter 2014

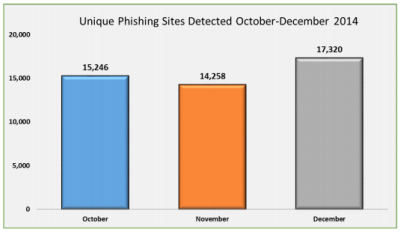
	October	November	December
Number of unique phishing websites detected	15,246	14,528	17,320
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	68,270	66,217	62,765
Number of brands targeted by phishing campaigns	271	273	300
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	44.88%	50.40%	50.37%
Percentage of sites not using port 80	0.72%	0.35%	1.04%

75

APWG Phishing Activity Trends (2014)

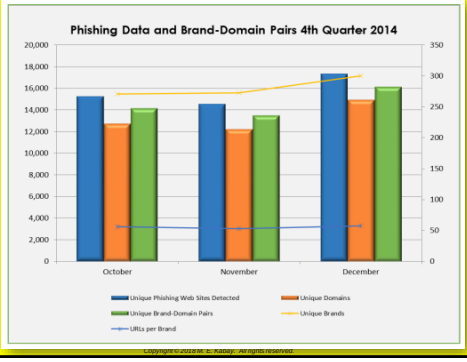
Phishing E-mail Reports and Phishing Site Trends – 4th Quarter 2014

The total number of unique phishing sites observed in Q4 was 46,824. This number is substantially lower than in Q3 by roughly half, a shift attributable to methodological refinements in how phishing sites were verified and URLs were de-duplicated to identify truly unique phishing sites. [See methology notes, p. 3.]



76

APWG Phishing Activity Trends (2014)

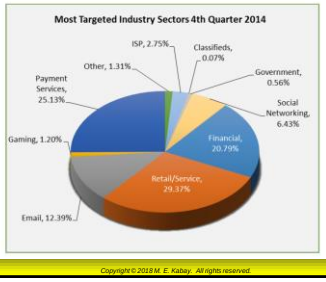


77

APWG Phishing Activity Trends (2014)

Most-Targeted Industry Sectors – 4th Quarter 2014

Retail/Service was the most-targeted industry sector in the fourth quarter of 2014, with 29.37 percent of phishing sites. Payment Services continued to be popular targets, with 29.37 percent of attacks during the three-month period.



78

APWG Phishing Activity Trends (2014)

Countries Hosting Phishing Sites – 4th Quarter 2014

The United States continued to be the top country where phishing sites were hosted during the third quarter of 2014. Phishers break into vulnerable web hosting to find hosting for the phishing sites, and the USA hosts a large percentage of the world's web sites.

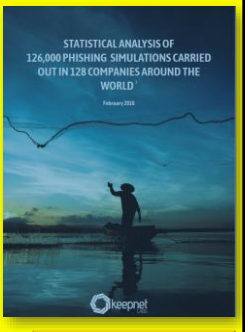
October		November		December	
United States	42.69%	United States	45.90%	United States	52.13%
Poland	7.60%	Poland	8.53%	United Kingdom	3.47%
China	5.96%	France	3.90%	Bulgaria	3.44%
Germany	3.96%	Germany	3.82%	Germany	3.42%
Russian Federation	3.57%	Netherlands	3.71%	France	2.83%
France	3.35%	United Kingdom	3.33%	Russian Federation	2.70%
Netherlands	2.95%	Turkey	2.66%	Turkey	2.64%
Canada	2.90%	Russian Federation	2.46%	Canada	2.48%
United Kingdom	2.85%	Canada	2.13%	Netherlands	2.04%
Turkey	2.23%	Hong Kong	1.60%	Brazil	1.87%

7

79

Keepnet Labs Phishing Simulation Study (2017) -- 1

- **~50% of employees in Legal, Audit, Internal Control, Mgmt, & IT will *open & read phishing emails***
- **~33% employees in Mgmt, in Legal, Audit, Internal Control, & R&D will *click a link in phishing emails***
- **~20% employees from R&D, Quality Mgmt, Health, & Sales will *respond to phishing emails by providing requested info***

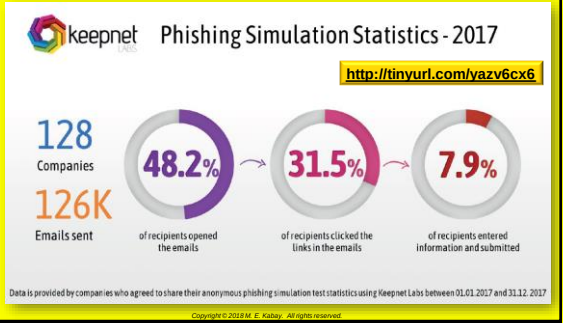


http://tinyurl.com/yazv6cx6

80

Keepnet Labs Phishing Simulation Study (2017) -- 2

- **Overall results for all departments**



81

Phish Fighting

- **Consumer education**
  - **E.g., Phishing Education Landing Page Program**
    - ✓ **Simple method to put educational page in place of 404 when phishing page taken down**
    - ✓ **http://education.apwg.org/r/about.html**
- **Fix email (will be a while)**
- **Blacklisting through browser**
- **Authenticate Web sites**
  - **SiteKey (see http://tinyurl.com/3mepsz)**
  - **SafePass mobile phone text messaging (see http://tinyurl.com/kneqax)**
  - **Token-based authentication instead of shared secrets (passwords & PINs)**

82

Trojans

- **Trojan Code**
- **Basic Anti-Trojan Tactics**
- **Lockdown & Quarantine**

83

Trojan Code

- **Trojan horse used by Greeks to trick Trojans into allowing soldiers hidden in belly of wooden statue into city**
- **Common Trojans include**
  - **Screensavers**
  - **Pornography**
- ***Trojan droppers* are programs that bundle Trojans along with harmless code**
  - **Typically in compressed archive**
  - **Created by *joiner* programs**
  - **May install components directly into RAM**
  - **Often used to install spyware / adware / viruses**
  - **See F-SECURE page at http://tinyurl.com/lgcblc**

84

Basic Anti-Trojan Tactics

- Well-educated users who don't
  - Execute random code
  - Open attachments from strangers
  - Open unexpected attachments even from known sources
- Keep operating systems and applications up to date: versions & patches
- Run good antimalware/antivirus ("AV") software at all times
- Scan system regularly using AV
- Beware messages claiming to be malware alerts – classic scam to trick users
- Don't fall for "scan-your-system-for-malware" ads

85

Lockdown & Quarantine

- Prevent unauthorized changes to code
- Prevent connections to unauthorized networks
- Scan all systems for safety before allowing connection; e.g., *Cisco Clean Access Agent*
  - Now called Cisco NAC (Network Admission Control) Appliance
  - http://www.cisco.com/en/US/products/ps6128/
  - Evaluates & remediates compliance with security policies; e.g.,
    - ✓Up-to-date AV strings
    - ✓Current patches
  - Blocks non-compliant systems

86

Now go and study

87