An Introduction to Protecting your (Mostly Online) Identity

Carlos Jensen
School of EECS
Oregon State University

cjensen@eecs...

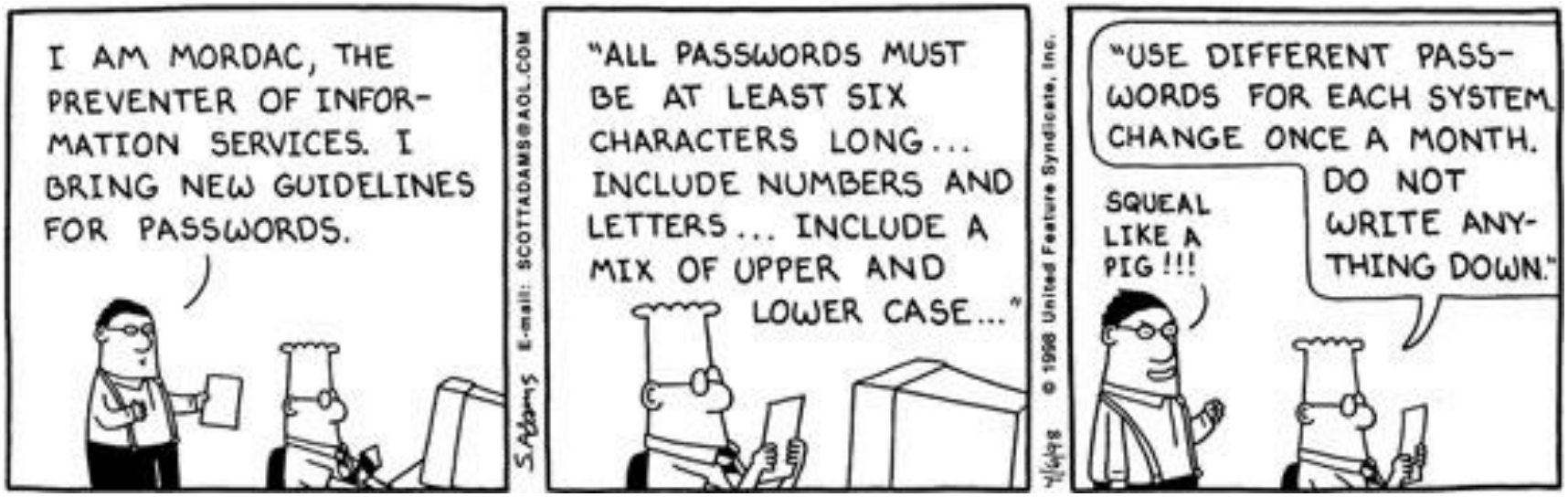
Overview

- Introduction to me & what I do
- Introduction/Background
  - What is Identify Theft
  - Who is at risk
  - Sources for Identity Theft
- Online Profiling and Identity Theft
  - Common techniques for Online Identity Theft
  - Common techniques for Online Profiling
- Discussion / Q&A

My Research – Usable Privacy & Security

Users characterized as #1 security vulnerability

- Users consistently and passionately express concern & interest
- Users consistently fail to act, or circumvents safeguards



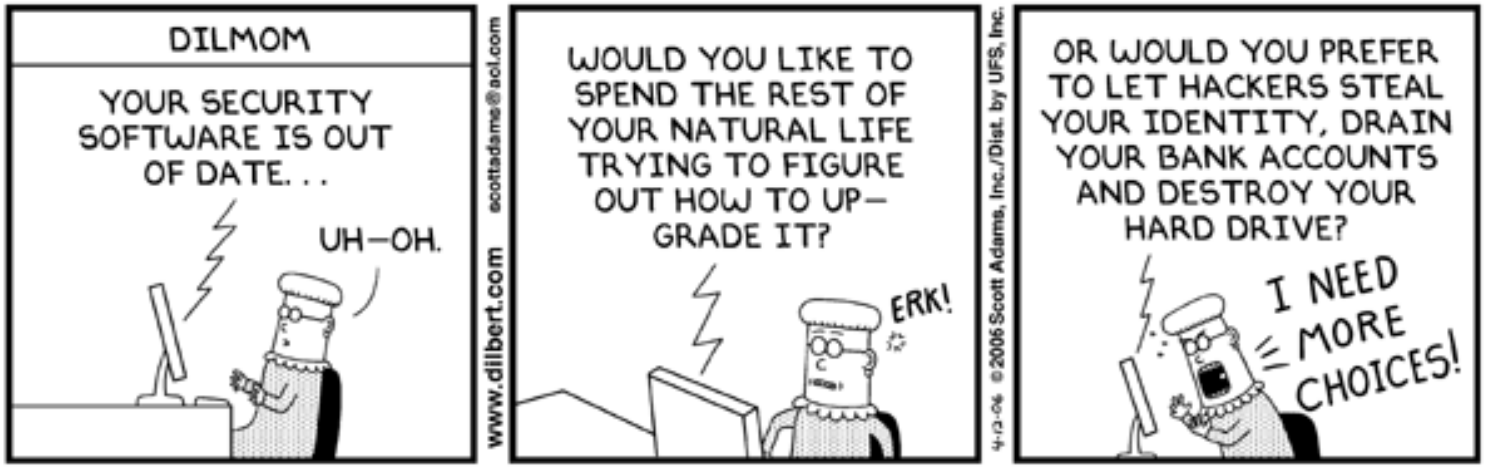
My Research – Usable Privacy & Security

Users often characterized as #1 security vulnerability

- Users consistently and passionately express concern & interest
- Users consistently fail to act, or circumvents safeguards

Root cause: Communication problems

- Giving users information and options that matter & make sense!

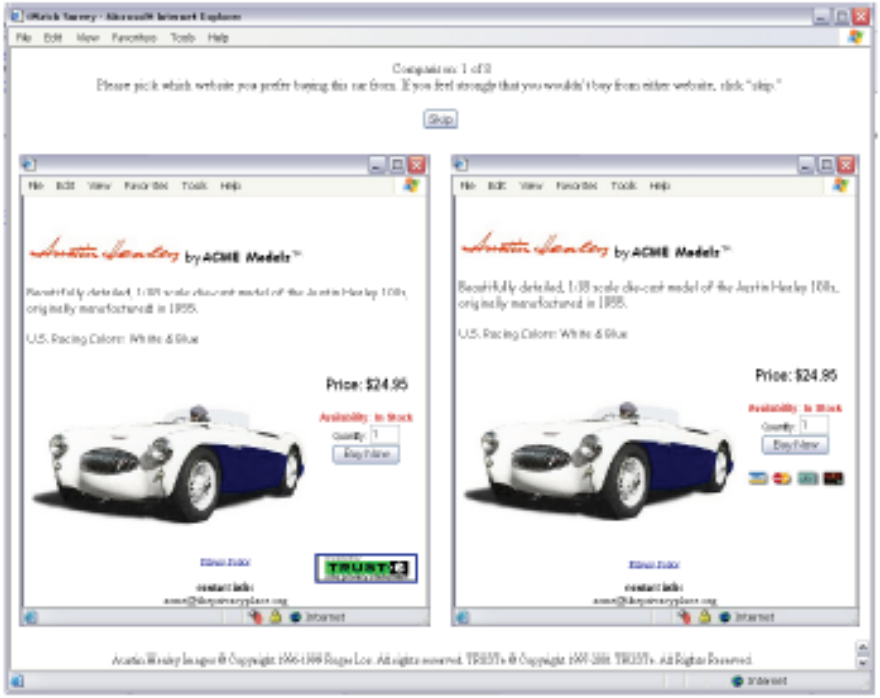


Understanding Users & Tools

User studies

- Actions vs. Intent
- Comprehension
- Interests & concerns

Impact of Policies & legislation



IEEE Security & Privacy
Int. Journal of Human Comp. Studies
ACM CHI

		P3P	Cookies	Web-bugs
Claim knowledge		21.5%	90.3%	34.8%
Demonstrate knowledge	Of above	25.0%	15.5%	17.2%
	Overall	5.4%	14.0%	5.4%

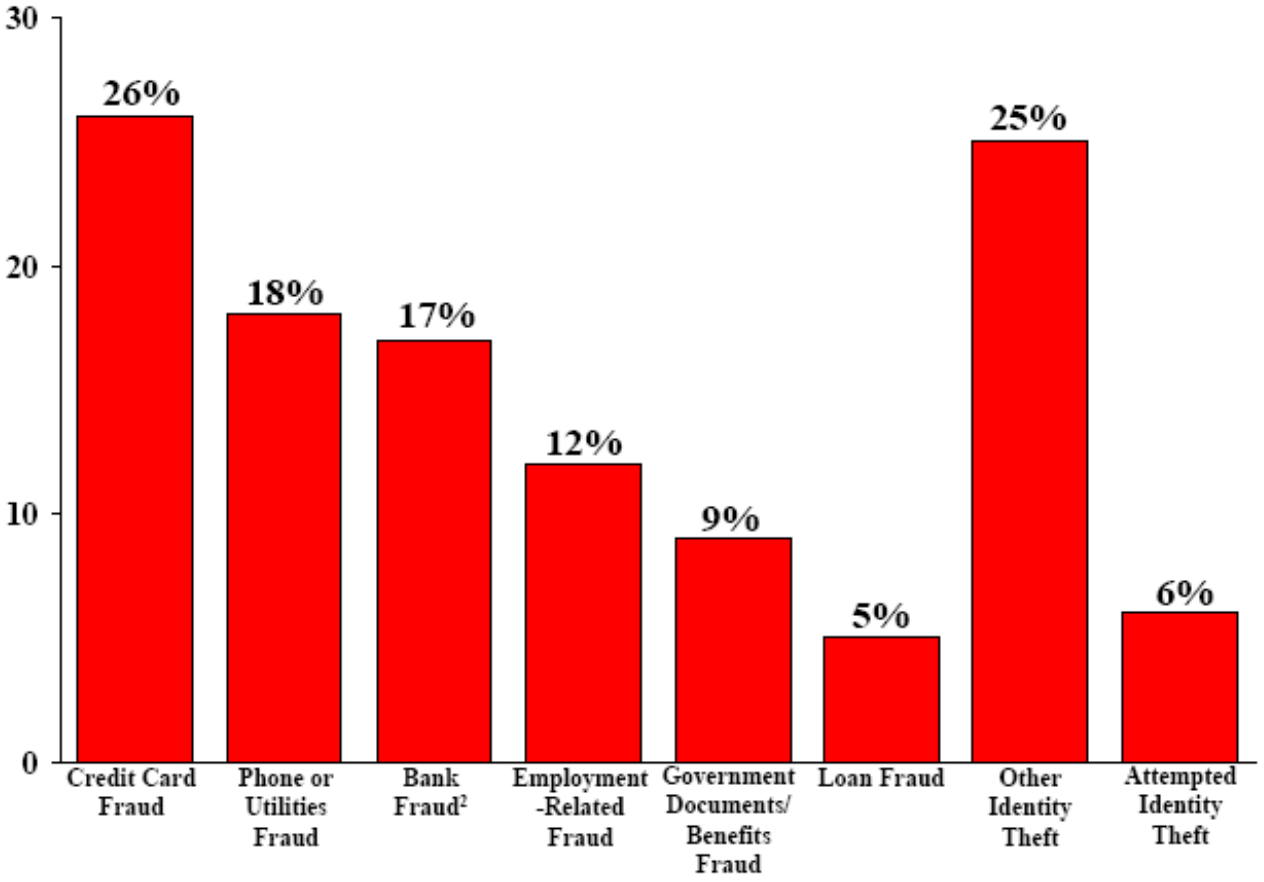
Identity Theft

What is Identity Theft?

"Identity theft and identity fraud are terms used to refer to all types of crime in which someone **wrongfully obtains and uses another person's personal data** in some way that involves fraud or deception, typically for economic gain." *U.S. Dept. of Justice*

http://www.usdoj.gov/criminal/fraud/idtheft.html

Types of Identity Theft



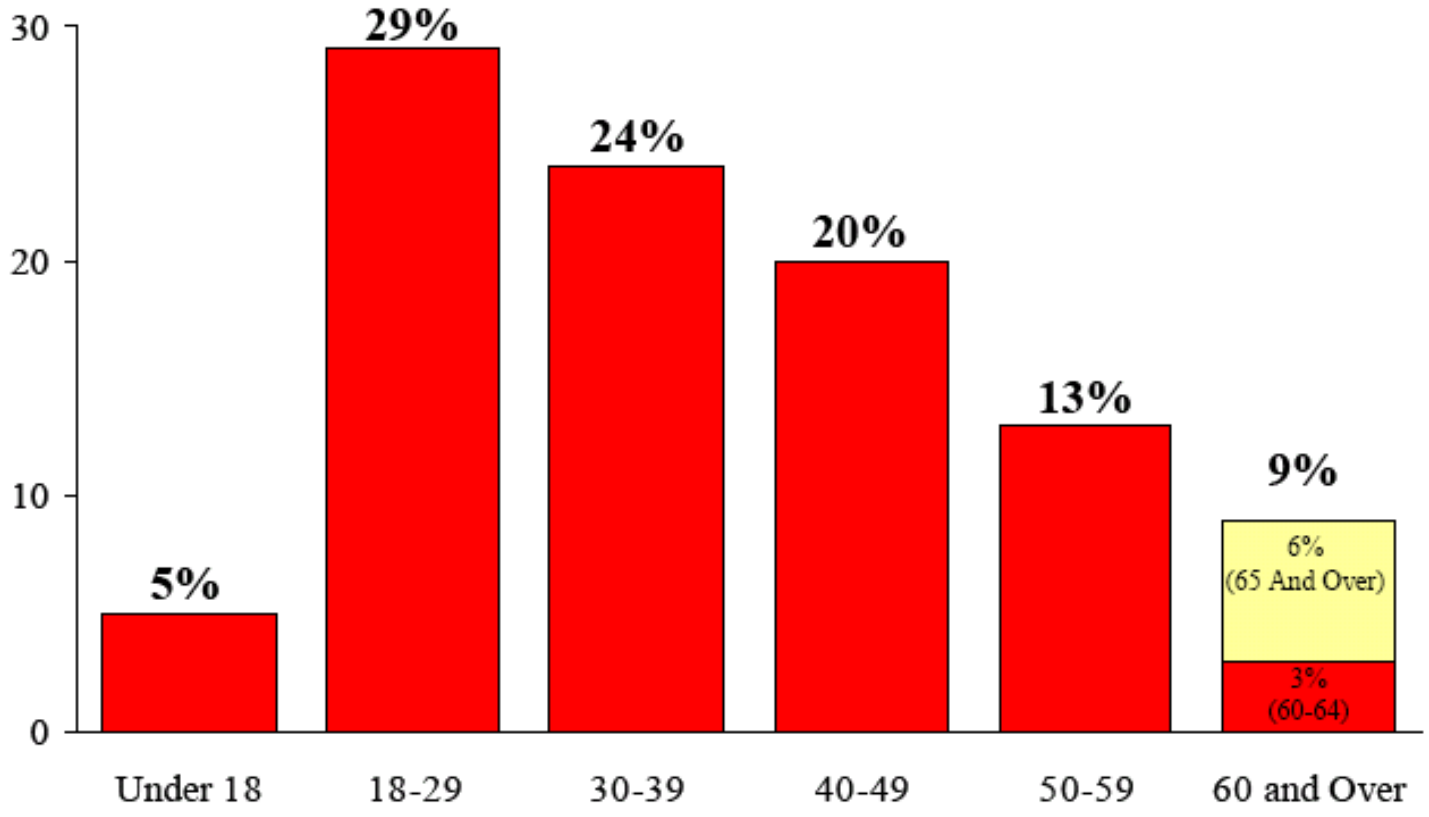
http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf

Types of Identity Theft

Goal is to assume your identity in order to commit:

- Credit card fraud
  - Open new accounts in your name
  - Hijack accounts
- Phone & Utilities fraud
- Bank/Finance fraud
  - Counterfeit checks
  - Opening new accounts and writing bad checks
  - Take out mortgages & car loans
- Government documents fraud

Who is at risk for Identity Theft



http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf

Who is at risk for Identity Theft

Rank	State	Victims per 1000 pop	Victims (in 1000's)
1	Arizona	5.5	362
2	Nevada	4.6	110
3	California	4.4	1,581
4	Texas	4.1	931
5	Colorado	3.4	158
6	Florida	3.3	596
7	Washington	3.2	203
8	New York	3.2	608
9	Georgia	3.0	277
10	Illinois	3.0	389
11	Maryland	3.0	169
12	New Mexico	3.0	57
13	Oregon	2.9	104
14	New Jersey	2.6	230
15	Michigan	2.5	249

Oregon high on statistics

Of these cases;

- 68.2% of ID theft off-line
- 11.6% of ID theft online
- 20.2% of unknown origin

The Cost of Identity Theft

Financial costs:

	# of victims	Average Loss	Total Loss
2005	8.4 million	$6,483	$56.6 Billion
2006	9.3 million	$6,278	$55.7 Billion
2007	10.1 million	$5,720	$49.3 Billion

Plus time to fix record (mean=25h, Avg=5hr)

http://www.privacyrights.org/ar/idtheftsurveys.htm

Commonly (miss)used information

- Name
- Address
- SSN's
- Family details

- Credit Card Numbers
- Email addresses
- Accounts
  - Entities
  - Types

- How dangerous is this information?

- How difficult is it to get this information?

Common “Causes” for Identity Theft

- Lost or stolen wallets
- Information misuse by family, friends, colleagues
- Dumpster diving
- Pretexting/social engineering
- Online scams & tracking
- Data brokers

The value of private information?

See http://turbulence.org/Works/swipe/calculator.html for cost of data from legitimate sources.

(Demo)

Black market: Credit card numbers with Mothers Maiden Name & codes: ~5% of available balance

World of Warcraft account details: $10.00

Online Privacy Threats

Online Identity Theft

Goal: Steal credit card or other financial or account information

Mechanisms:

- Phishing (email)
  - Trojans, worms, viruses
- Spyware
- Server Hacks

Online Profiling

Goal: Track your activities Online, including what you do, and who you interact with

Mechanisms:

- Cookies
- Webbugs
- Deceptive/Abusive data practices

Spam & Phishing

Spam & Phishing

Spam is unsolicited commercial email

Phishing attacks are email messages aimed at tricking you into revealing some valuable information

- Submitting credit card numbers
- Submitting account information (user name, password)

Phishing – Sent randomly, hoping people will bite

Spear-Phishing – Targeted phishing attacks

Puddle-Phishing – Targeting small communities

Phishing

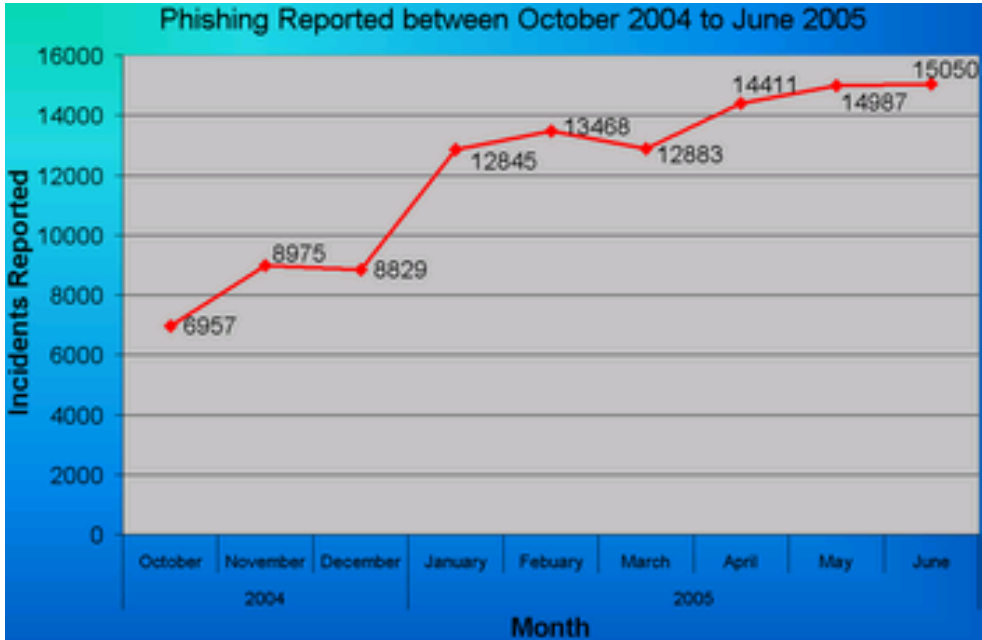
Dear ORST Webmail Subscriber,

We notice that your webmail account has been compromised by spammers.They have gained access to your webmail account and have been using it for illegal internet activities.You are to send us your account information immediately to enable us reset your account.A new password will be sent to you once this is done.Send the information as follows

*User Name:
*Password:

You are advised to send this information immediately or we will delete your acocunt from our network.

THE ORST HELP DESK



Anatomy of Phishing

```
Oct 21 09:10:48 2008
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <helpdsk@orst.edu>
Received: from smtp5.oregonstate.edu (smtp5.oregonstate.edu [128.193.15.33])
        by tok.eecs.oregonstate.edu (8.14.0/8.14.0) with ESMTP id m89DNhEW016663
        for <cjensen@eecs.oregonstate.edu>; Tue, 9 Sep 2008 06:23:43 -0700 (PDT)
Received: from localhost (localhost [127.0.0.1])
        by smtp5.oregonstate.edu (Postfix) with ESMTP id 7CCAA4103EF;
        Tue,  9 Sep 2008 06:23:43 -0700 (PDT)
X-Virus-Scanned: amavisd-new at oregonstate.edu
X-Spam-Flag: NO
X-Spam-Score: 0
X-Spam-Level:
X-Spam-Status: No, score=0 tagged_above=-999 required=5 tests=[none]
Received: from smtp5.oregonstate.edu ([127.0.0.1])
        by localhost (smtp.oregonstate.edu [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id oS115ZC+qYRs; Tue,  9 Sep 2008 06:23:41 -0700 (PDT)
Received: from mr4.cc.emory.edu (mr4.cc.emory.edu [170.140.52.93])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by smtp5.oregonstate.edu (Postfix) with ESMTP id 084204103B6;
        Tue,  9 Sep 2008 06:21:59 -0700 (PDT)
Received: from localhost (emoryfloatdmz.cc.emory.edu [170.140.52.254])
        by mr4.cc.emory.edu (8.13.1/8.13.1) with ESMTP id m89DLsOS005277;
        Tue, 9 Sep 2008 09:21:55 -0400
Received: from dial-pool11.ph.starcomms.net (dial-pool11.ph.starcomms.net
        [41.205.168.161]) by webmail.service.emory.edu (Horde MIME library) with
        HTTP; Tue, 09 Sep 2008 09:21:52 -0400
Message-ID: <20080909092152.gghsnom1xcw840g0@webmail.service.emory.edu>
Date: Tue, 09 Sep 2008 09:21:52 -0400
From: THE ORST HELP DESK <helpdsk@orst.edu>
Reply-to: helpdsk@info.lt
To: undisclosed-recipients:;
Subject: Webmail Update
MIME-Version: 1.0
Content-Type: text/plain;
        charset=ISO-8859-1;
        format="flowed"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
User-Agent: Internet Messaging Program (IMP) H3 (4.0.5)
X-emory.edu-MailScanner: Found to be clean
X-emory.edu-MailScanner-SpamScore: s
X-emory.edu-MailScanner-From: helpdsk@orst.edu
```

Email gets passed from one server to the next until it reaches destination.

Can (sometimes) be traced

This is the information your email program will give you about this message, if you really really want.

Overwhelmed yet?

Anatomy of Phishing

Oct 21 09:10:48 2008
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <helpdsk@orst.edu>
Received: from smtp5.oregonstate.edu (smtp5.oregonstate.edu [128.193.15.33])
by tok.eecs.oregonstate.edu (8.14.0/8.14.0) with ESMTP id m89DNhEW016663
for <cjensen@eecs.oregonstate.edu>; Tue, 9 Sep 2008 06:23:43 -0700 (PDT)
Received: from localhost (localhost [127.0.0.1])
by smtp5.oregonstate.edu (Postfix) with ESMTP id 7CCAA4103EF;
Tue, 9 Sep 2008 06:23:43 -0700 (PDT)
X-Virus-Scanned: amavisd-new at oregonstate.edu
X-Spam-Flag: NO
X-Spam-Score: 0
X-Spam-Level:
X-Spam-Status: No, score=0 tagged_above=-999 required=5 tests=[none]
Received: from smtp5.oregonstate.edu ([127.0.0.1])
by localhost (smtp.oregonstate.edu [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id 0St5ZC+qfRs; Tue, 9 Sep 2008 06:23:41 -0700 (PDT)
Received: from mr4.cc.emory.edu (mr4.cc.emory.edu [170.140.52.93])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(No client certificate requested)
by smtp5.oregonstate.edu (Postfix) with ESMTP id 084204103B6;
Tue, 9 Sep 2008 06:21:59 -0700 (PDT)
Received: from localhost (emoryfloatdmz.cc.emory.edu [170.140.52.254])
by mr4.cc.emory.edu (8.13.1/8.13.1) with ESMTP id m89DLsOS005277;
Tue, 9 Sep 2008 09:21:55 -0400
Received: from dial-pool11.ph.starcomms.net (dial-pool11.ph.starcomms.net
[41.205.168.161]) by webmail.service.emory.edu (Horde MIME library) with
HTTP; Tue, 09 Sep 2008 09:21:52 -0400
Message-ID:
<20080909092152.gghsnom1xcw840go@webmail.service.emory.edu>
Date: Tue, 09 Sep 2008 09:21:52 -0400
From: THE ORST HELP DESK <helpdsk@orst.edu>
Reply-to: helpdsk@info.lt
To: undisclosed-recipients:;
Subject: Webmail Update
MIME-Version: 1.0
Content-Type: text/plain;
charset=ISO-8859-1;
format="flowed"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
User-Agent: Internet Messaging Program (IMP) H3 (4.0.5)
X-emory.edu-MailScanner: Found to be clean
X-emory.edu-MailScanner-SpamScore: s
X-emory.edu-MailScanner-From: helpdsk@orst.edu

The important pieces

<- OSU didn't think this was spam

<- Message came via Emory University

<- Message came via Emory University

<- Message came from dialup modem!

<- Server reference for message

<- Note discrepancy!!!

<-

Anatomy of Phishing

Oct 21 09:10:48 2008
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <helpdsk@orst.edu>
Received: from smtp5.oregonstate.edu (smtp5.oregonstate.edu [128.193.15.33])
by tok.eecs.oregonstate.edu (8.14.0/8.14.0) with ESMTP id m89DNhEW016663
for <cjensen@eecs.oregonstate.edu>; Tue, 9 Sep 2008 06:23:43 -0700 (PDT)
Received: from localhost (localhost [127.0.0.1])
by smtp5.oregonstate.edu (Postfix) with ESMTP id 7CCAA4103EF;
Tue, 9 Sep 2008 06:23:43 -0700 (PDT)
X-Virus-Scanned: amavisd-new at oregonstate.edu
X-Spam-Flag: NO
X-Spam-Score: 0
X-Spam-Level:
X-Spam-Status: No, score=0 tagged_above=-999 required=5 tests=[none]
Received: from smtp5.oregonstate.edu ([127.0.0.1])
by localhost (smtp.oregonstate.edu [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id 0St5ZC+qYRs; Tue, 9 Sep 2008 06:23:41 -0700 (PDT)
Received: from mr4.cc.emory.edu (mr4.cc.emory.edu [170.140.52.93])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(No client certificate requested)
by smtp5.oregonstate.edu (Postfix) with ESMTP id 084204103B6;
Tue, 9 Sep 2008 06:21:59 -0700 (PDT)
Received: from localhost (emoryfloatdmz.cc.emory.edu [170.140.52.254])
by mr4.cc.emory.edu (8.13.1/8.13.1) with ESMTP id m89DLsOS005277;
Tue, 9 Sep 2008 09:21:55 -0400
Received: from dial-pool11.ph.starcomms.net (dial-pool11.ph.starcomms.net
[41.205.168.161]) by webmail.service.emory.edu (Horde MIME library) with
HTTP; Tue, 09 Sep 2008 09:21:52 -0400
Message-ID:
<20080909092152.gghsnom1xcw840go@webmail.service.emory.edu>
Date: Tue, 09 Sep 2008 09:21:52 -0400
From: THE ORST HELP DESK <helpdsk@orst.edu>
Reply-to: helpdsk@info.lt
To: undisclosed-recipients:;
Subject: Webmail Update
MIME-Version: 1.0
Content-Type: text/plain;
charset=ISO-8859-1;
format="flowed"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
User-Agent: Internet Messaging Program (IMP) H3 (4.0.5)
X-emory.edu-MailScanner: Found to be clean
X-emory.edu-MailScanner-SpamScore: s
X-emory.edu-MailScanner-From: helpdsk@orst.edu

- Your spammers were operating out of Latvia (maybe)
- Was Emory helping them?
- Does the sending computer belong to the spammers?
- The role of Bot-nets, viruses & worms

Why Phishing Works

In 2003 approximately 2 million people gave away information in phishing attacks (5% of recipients) valued at $1.2 billion

90% of study participants fooled by good phishing sites

http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

Why Phishing Works

Common techniques

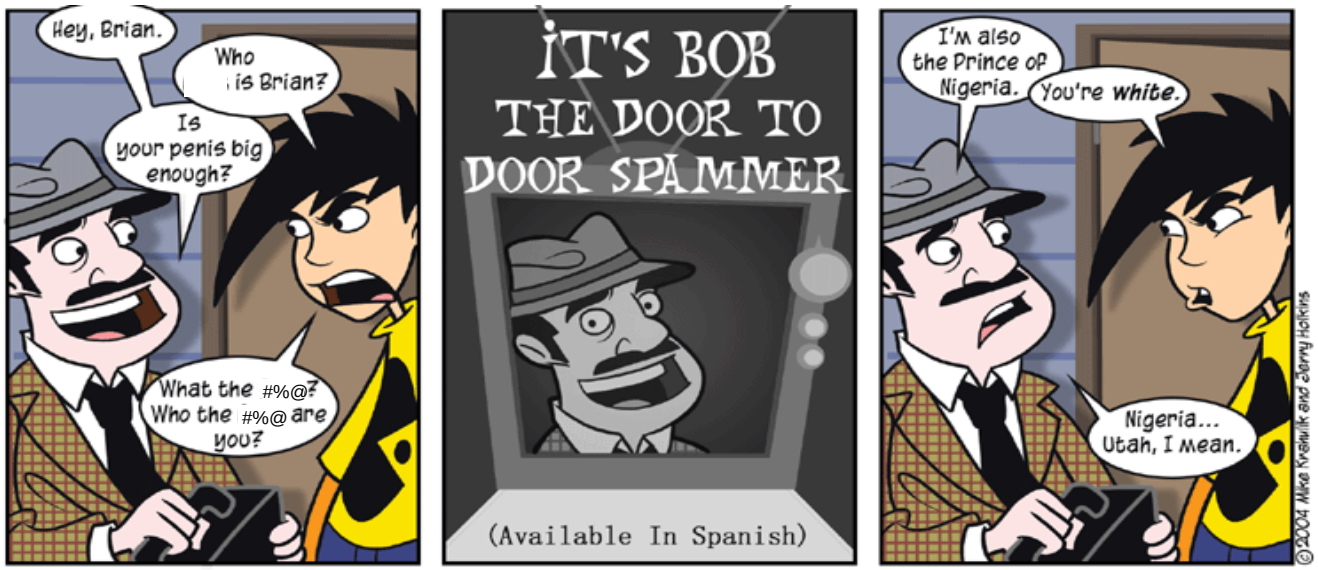
- Address obfuscation for links
  - www.cilibank.com
  - www.ebay-security.com
  - www.capitalone.com
- Visual deception
  - Emails, logos and sites that look real
  - Bring up real site in addition to fake login box

http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

Surviving Phishing Attacks

- Don't follow links from email
- Don't download files from email
- Keep an up-to-date spam filter

- Use common sense!
  - If it sounds too good/bad to be true… It probably is



More Information at: http://www.antiphishing.org/resources.html

Spyware

Spyware is software installed on your machine which **secretly tracks your activities**, such as:

- All the websites you visit
- All the characters you type (keylogger)

and later transmitted to a third party for either **target advertising** or **theft** of passwords and financial information

Spyware

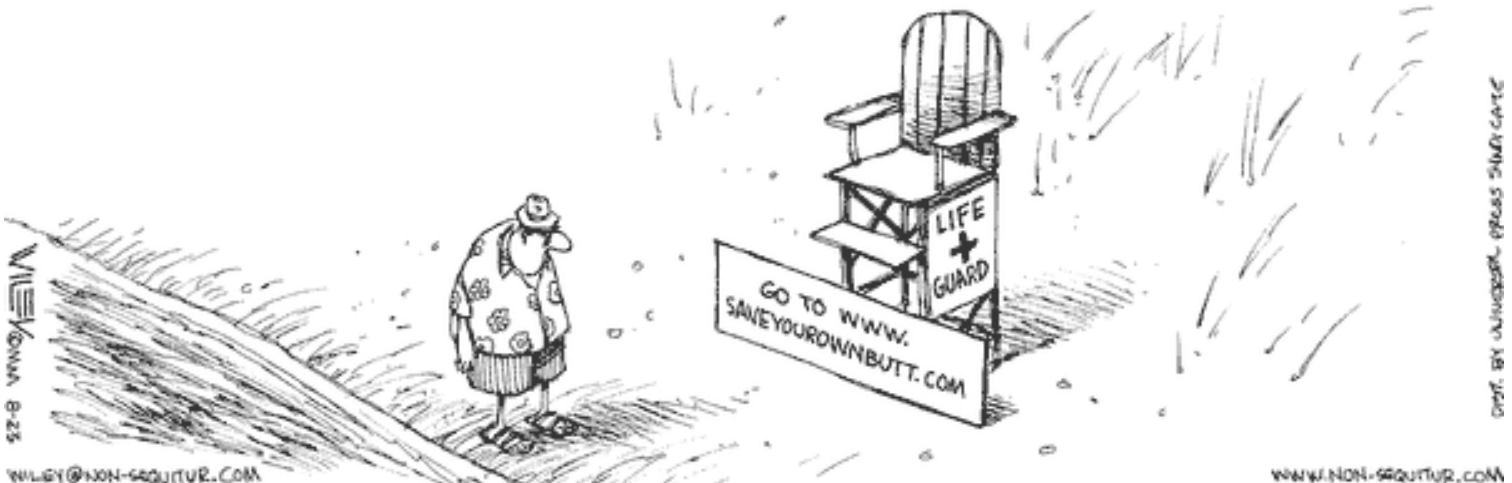
Route of entry:

- User installation
  - False advertising & deception
    - Software promises to do one thing, in addition tracks
    - Often promise to fight spyware or viruses!
    - Often attached to shareware and P2P software
    - Toolbars for browsers
  - Examples
    - 180 solutions
    - RedSherriff

- Stealth installation
  - Take advantage of holes in security or browser
  - Aka. Drive-by Installation

Who is Responsible?

- You!
- Get help from:
  - Federal Trade Commission
  - Credit Card issuer/Bank
  - Internet Service Provider



Online Profiling

While not as bad as identity theft, can still be damaging, and often used together

Two main mechanisms:

- Cookies (3rd party)
- Webbugs

Both (potentially) enable a 3rd party to see where you go

See http://www.epic.org/privacy/profiling/ for dangers of profiling

Glossary

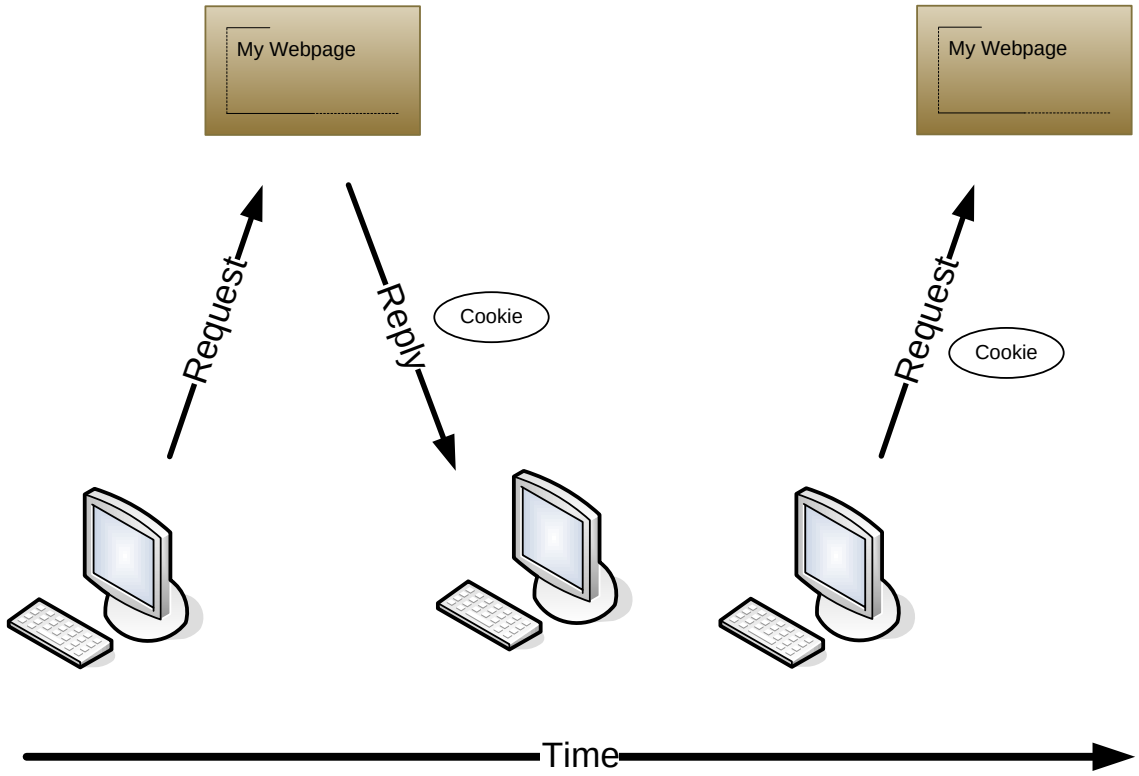
Cookies

- Text files saved on your computer to allow a given server to "remember" you
- Can only be read by **specified** server
- Can be set by any "page" you go to
  - Session cookies
  - 1st party cookies
  - 3rd party cookies

Webbugs

- Used both in Spam and web pages
- 1x1 pixel transparent images used to contact a 3rd party server to notify it that you have visited the page, or read the email
- Aka web-beacon, tracking bug, pixel tag, PattyMail

How cookies work

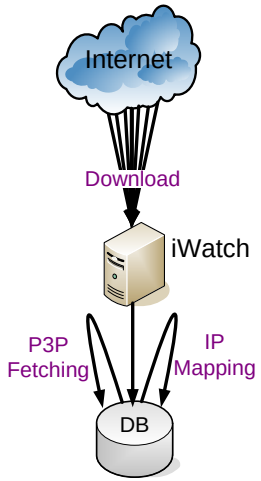


- Session cookies disappear when you close your browser
- 1st party cookies are set for you, by you
- 3rd party cookies are set for someone else to pick up

Demo: Tamper Data (Firefox)

Tamper Data is a plug-in for Firefox which lets you review & manipulate what information flows between your computer & websites

The iWatch Web-crawler



iWatch web-crawler catalogues online data collection and practices such as:

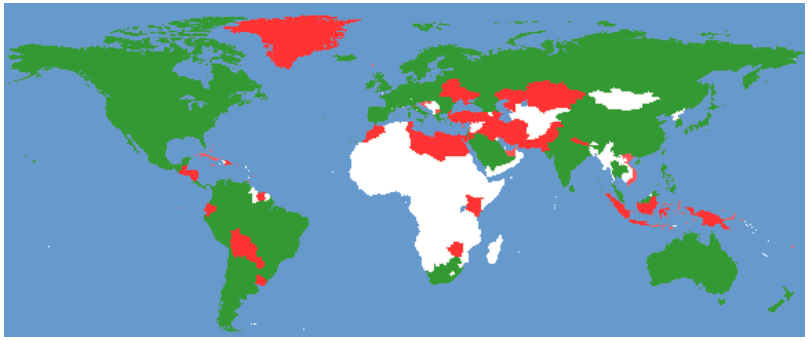
- Cookies,
- Webbugs,
- Popups,
- Banner Advertising,
- Privacy Policies and Seals

iWatch supports the study of:

- Evolution of practices over time
- Geographic and industry trends
- Technology adoption and impact

Provide data to aid

- Consumers
- Legislators
- E-merchants
- Researchers



	May 05	Aug 06	May 07	Total
Pages	119,237	121,103	377,728	618,068
Domains	15,792	10,421	27,392	53,605
Pages/Domain	7.55	11.22	13.78	11.53
Countries	43	43	59	60
Domains/Country	367.26	242.35	462.27	893.42

Internet Forensics

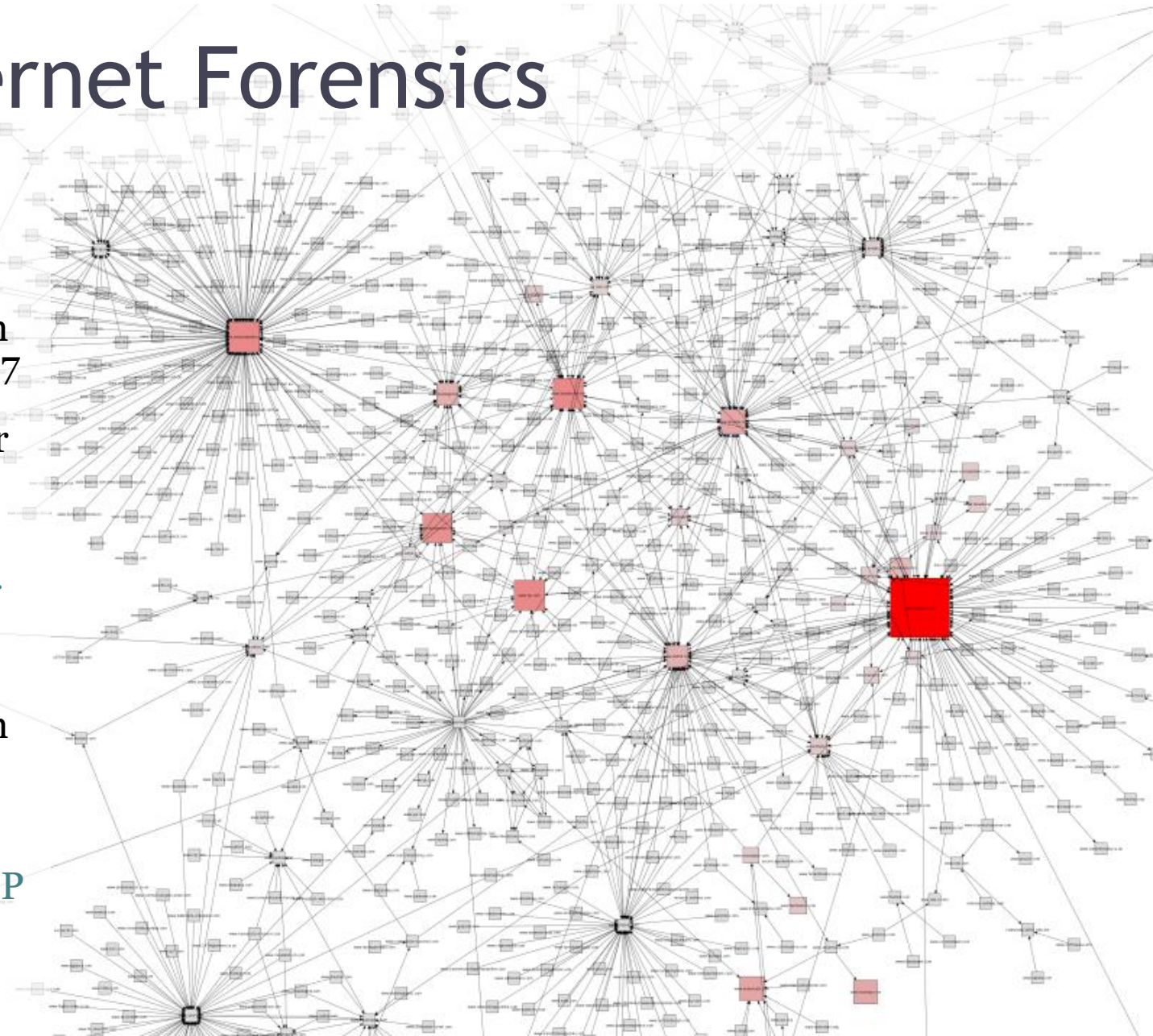
Going beyond surface statistics

What happens when the website and 1007 of its closest friends decide to share their data?

Node size and color indicates amount of data collected

What happens when sites lie in their policies?

27% of sites with P3P policies fail to disclose cookie use



Top 20 3rd Party-Resource Servers

1. graphics.fansonly.com
2. graphics.ocsn.com
3. server-au.imrworldwide.com
4. i.cmpnet.com
5. welcome.hp-ww.com
6. www.qksrv.net
7. dw.com.com
8. pics.ebaystatic.com
9. server-dk.imrworldwide.com
10. ehg-dig.hitbox.com
11. server-us.imrwordwide.com
12. pagead2.googlesyndication.com
13. switch.atdmt.com
14. hostingprod.com
15. ehg-findlaw.hitbox.com
16. view.atdmt.com
17. incude.ebaystatic.com
18. images.findlaw.com
19. ads.api.no
20. ad.doubleclick.net

Of the top 20 3rd party-resource servers:

70% are ad-servers or marketers

30% are dedicated image or script servers