Hidden Universes / Security and Privacy Issues

DANGER
PHISHING SCAM

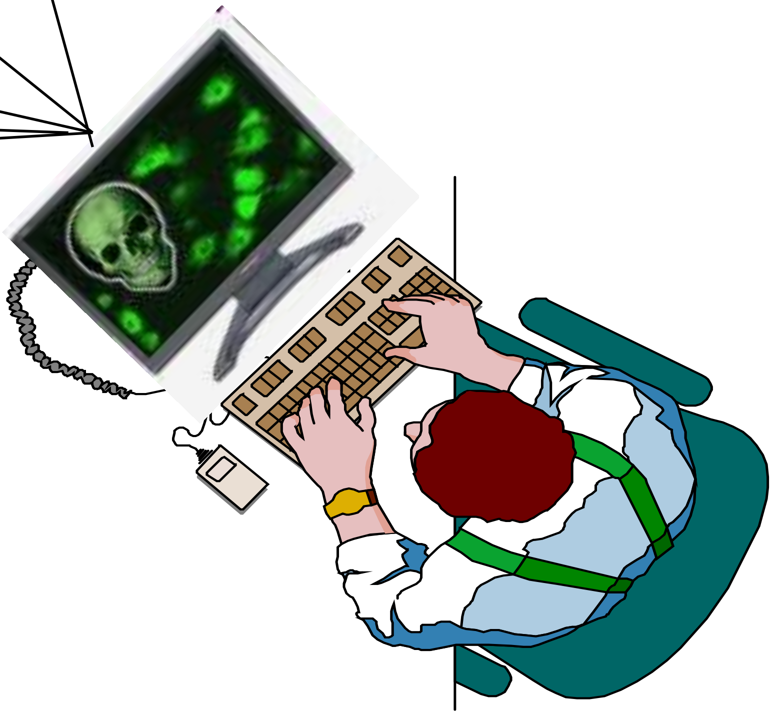
Find us on Facebook

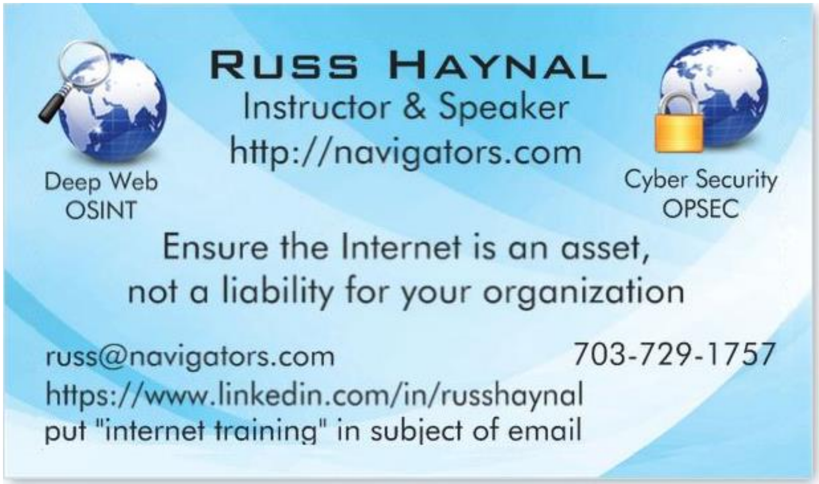
THE INTERNET OF THINGS

Day #3

Free WiFi spot

Google Analytics





Russ Haynal
Instructor & Speaker
http://navigators.com

Deep Web
OSINT

Cyber Security
OPSEC

Ensure the Internet is an asset,
not a liability for your organization

russ@navigators.com 703-729-1757
https://www.linkedin.com/in/russhaynal
put "internet training" in subject of email

Revision 04/2024

Note: If you send me an email, put “internet training” in the e-mail's subject

Security and Privacy Issues

1. Background and Statistics
2. Network connections (at work and home)
3. Firewalls, Anti-Virus
4. “Persona” details and options
5. Tracking you cyber: web browser, email, social media
6. Tracking you physical: phone, internet of things
7. Critical Advice and Summary

Online web page = http://navigators.com/issues.html

An Opening Survey

- What type of Internet connection(s) do you have:
  - attributable (agency.gov, yourcompany.com), mis-attributable, home
- Have you researched work-related topics via your home account?
- Is there a WIFI network in your SCIF?
- Is there a WIFI network in your home?
- Do you access the Internet at home without a firewall?
- Do you, or anyone in your extended family, use a genealogy program (e.g. Family Tree Maker)
- Do you, or anyone in your family, use social media?
- Have you ever clicked on an email link or attachment?
- What apps in your phone can access GPS / wifi / bluetooth?
- How many microphones are in your house? Are you sure?

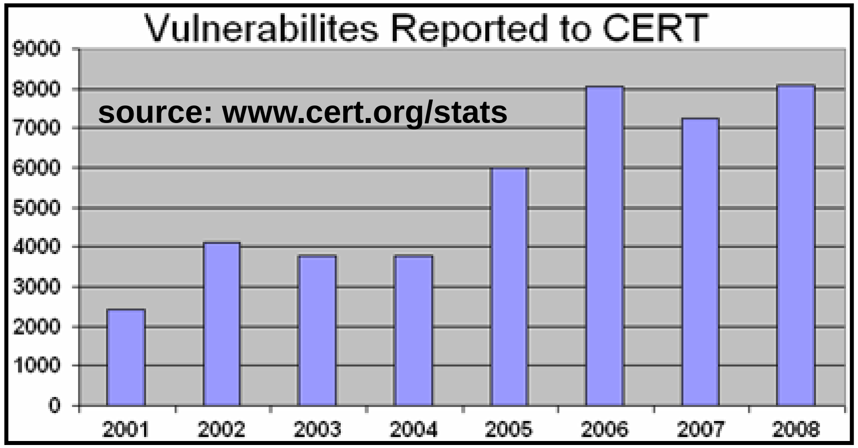
Why this Session…

- This session covers a variety of security and privacy issues
- Many issues apply directly to work-related Internet usage
- Some issues apply strictly to home/mobile Internet usage
- These issues are important from a counter-intelligence perspective
  - Minimize “leaking” of your research interests
  - Protection of your personal information and identity
- If security of your personal Internet devices are breached, you could be in a compromised/vulnerable situation

Internet = Passport to interact with foreign resources and people

These historic stats are based on PC's History is repeating with 'Internet of things"

Russ Haynal
Internet Instructor & Speaker
http://navigators.com/
privacy.html

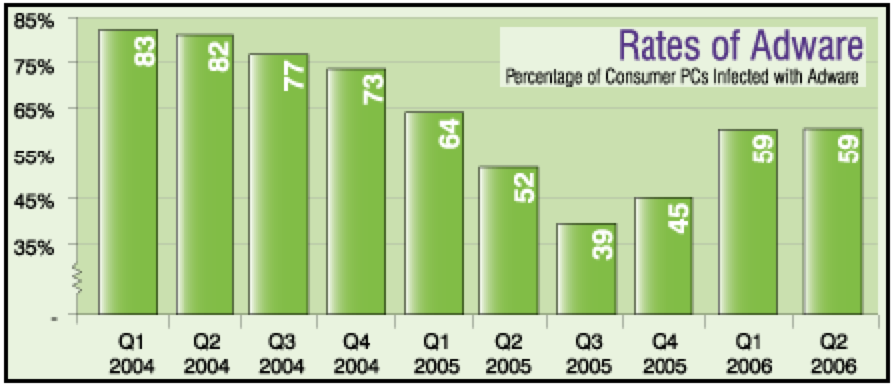


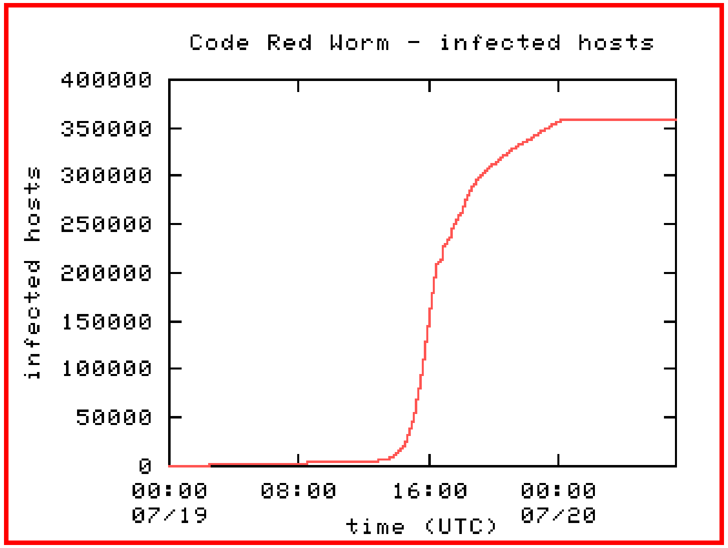
source: www.cert.org/stats

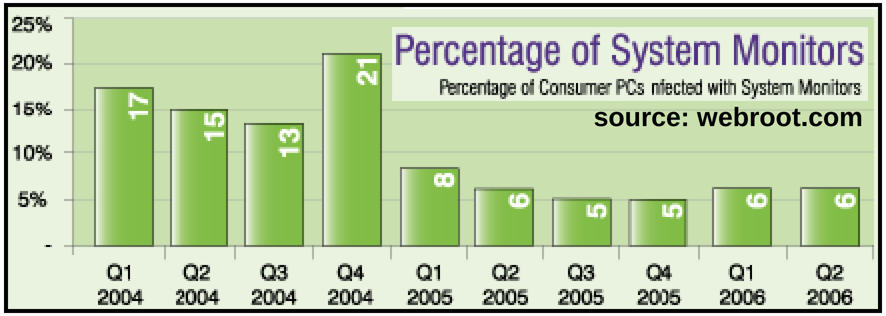
Privacy Practices of Web Domains

	Random Sample	Top 100 Popular
Collect Personally Identifiable Information	90%	96%
Places Third Party Cookies	28%	48%
Posts Privacy Statement	88%	98%
Displays Privacy Seal (ie. Truste, BBB)	12%	44%

Source:http://www.pff.org/publications/privacyonlinefinalael.pdf







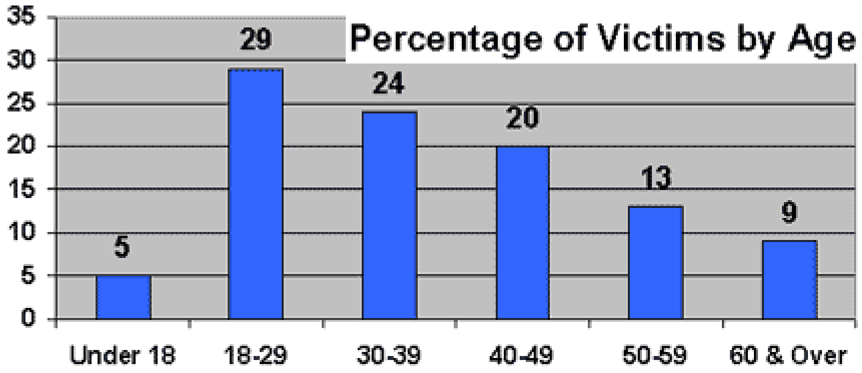
source: webroot.com

http://www.caida.org/analaysis/security

Identity Theft

12 million victims annually in the U.S. Average loss = $5,130
100+ million user records stolen (Target, Anthem, OPM, Equifax)

- **Identity theft occurs when someone has collected enough personal information about you, that they can "impersonate" you**
- **They access your existing financial accounts, investment accounts**
- **They establish <u>new</u> accounts (checking, credit card, loans)**
- **They collect your personal Information through traditional means – dumpster diving, scam solicitations, corrupt employee.**
- **Hacker gains access to your PC: account #'s, investment software, cookies, auto-complete password, and family genealogy**
- **Researches Facebook and public databases**



Free credit report every 12 months from each of the 3 credit bureaus

Annualcreditreport.com or call 1-877-322-8228

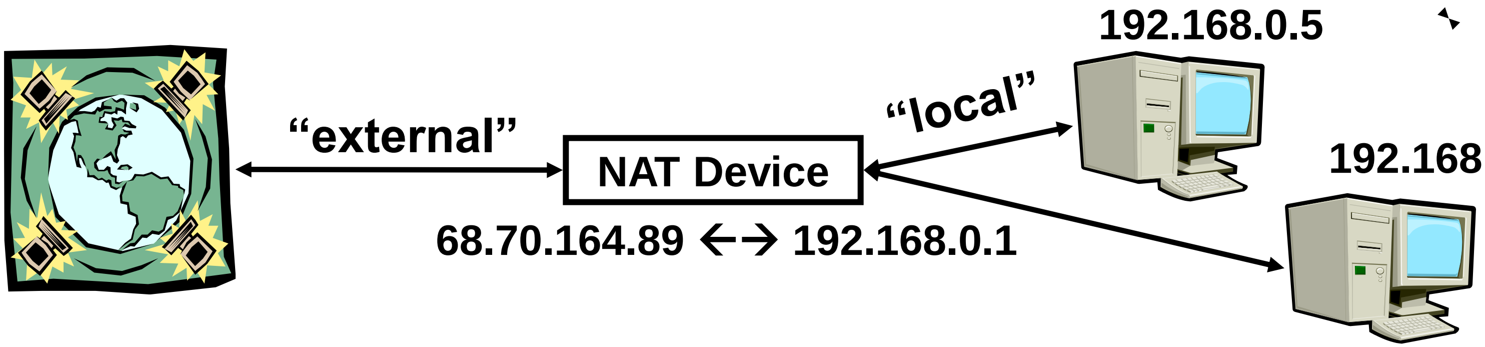
Internet Connection Definitions

- **IP address - Internet Protocol address allocated to you from your ISP**
- **Fixed IP address - the same IP address remains permanently assigned**
- **Dynamically assigned IP address – During a log-in/connect sequence, an IP address is assigned for the duration of that session.**
  Such IP addresses may be assigned from a “DHCP” Host
  (Dynamic Host Configuration Protocol)
- **Dial-up – only connected part-time.**
  Dial-up accounts received dynamically assigned IP address
- **Broadband – FIOS /Cable/DSL Connected 24 X 7**
  A broadband account may receive a fixed or dynamic IP address
  A dynamic IP address may persist for a very long time

Network Address Translation

- NAT is the translation of an IP address from one network segment into an IP address that is used on another network segment
- NAT is often used where a private network touches a public network e.g. Internet → broadband modem → local network
- Certain IP addresses are reserved for use on private networks (reference: RFC's 1918, 1631)

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255



"external"

NAT Device

68.70.164.89 ←→ 192.168.0.1

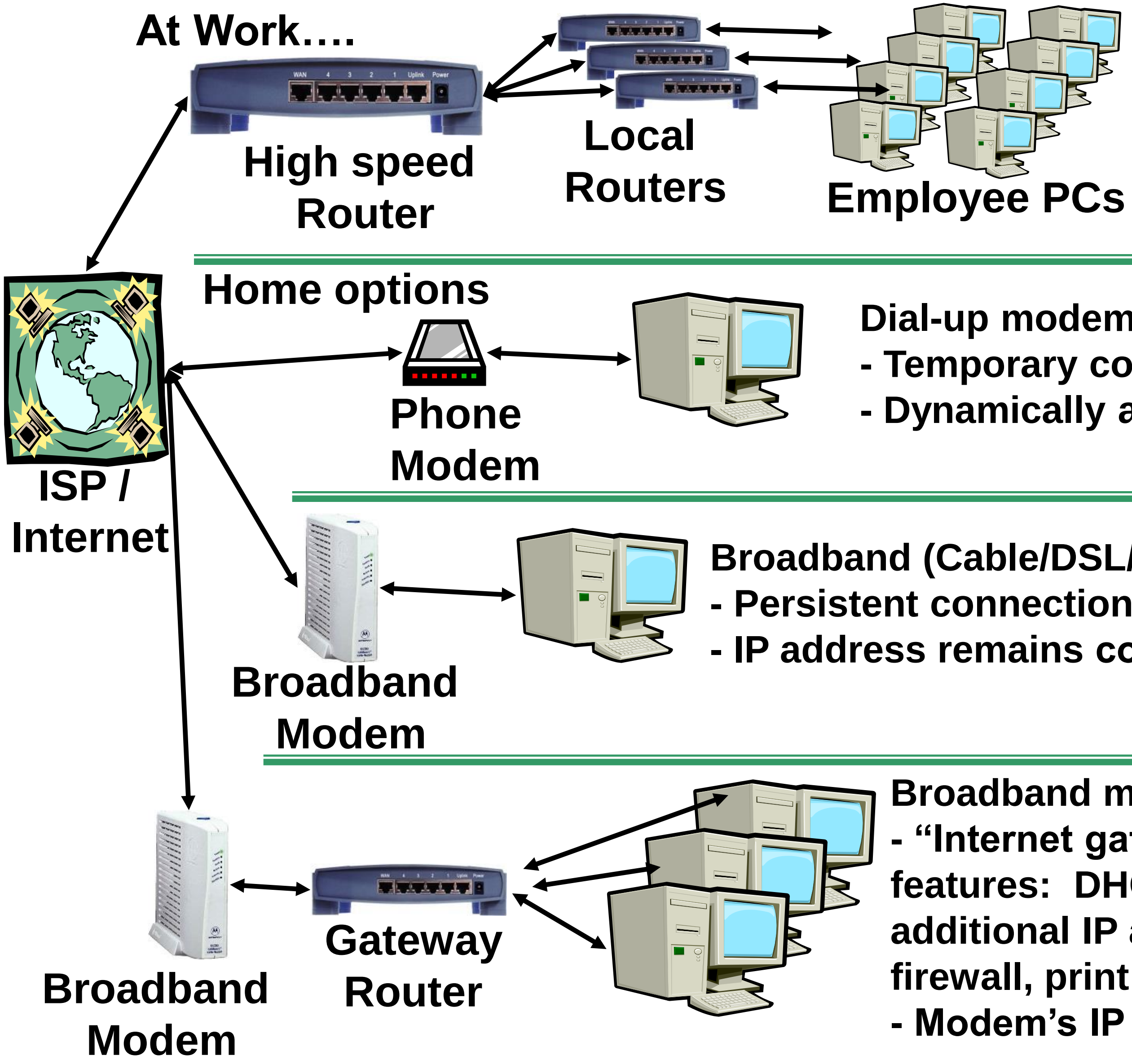
"local"

192.168.0.5

192.168.0.83

- To see your "external" IP address: "check your persona" on my web site
- To see your computer's "local" IP address: DOS prompt → ipconfig /all

Getting Online…



Wide variety of implementations including firewalls.

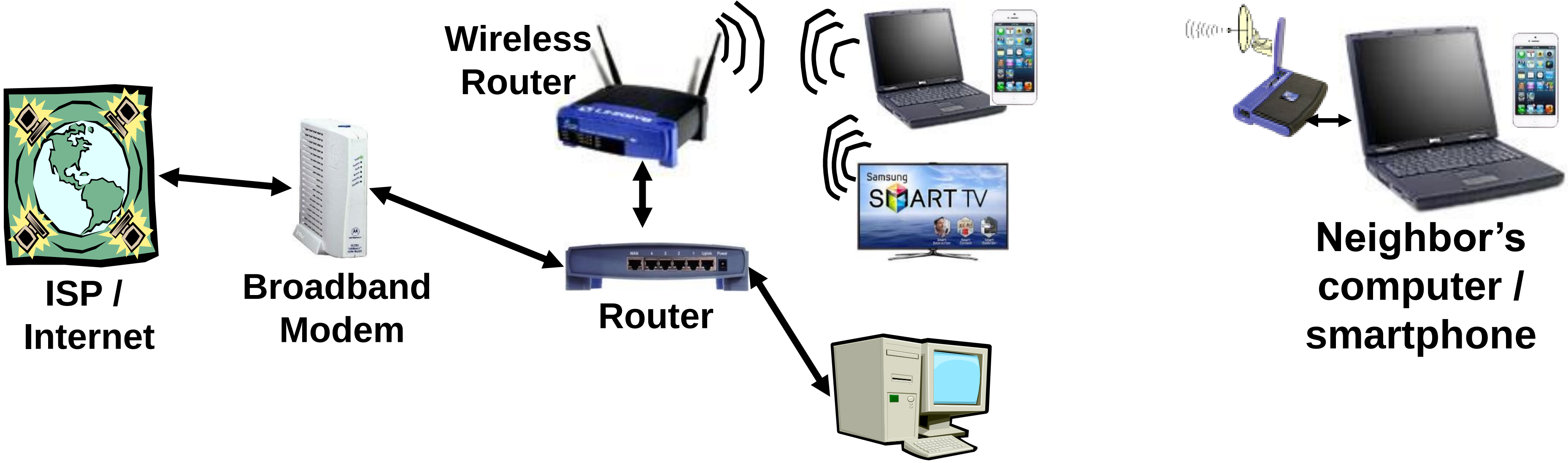
Dial-up modem with a single PC
- Temporary connection
- Dynamically assigned IP number

Broadband (Cable/DSL/fiber) with a single PC
- Persistent connection
- IP address remains constant throughout "session"

Broadband modem with multiple PCs
- "Internet gateway router" includes extra features: DHCP and NAT to assign additional IP addresses to all computers; firewall, print server, wireless
- Modem's IP address = Internet persona

A special note about wireless networks (are you sure, you can't install a wire?)

- **Remote "guests" may connect into your local network**
- **Wireless networking standards are always evolving:**
  802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax
- **WEP (Wireless Equivalent Privacy) has a weakness in its algorithm.**
  WEP can easily be compromised using free shareware
  WPA / WPA2 / WPA3 (WIFI Protected Access) adds security



Comcast Modems are now Public WIFI Hotspots!

Read the manual for your router and UPDATE the firmware

Security and Privacy Issues

1. Background and Statistics
2. Network connections (at work and home)

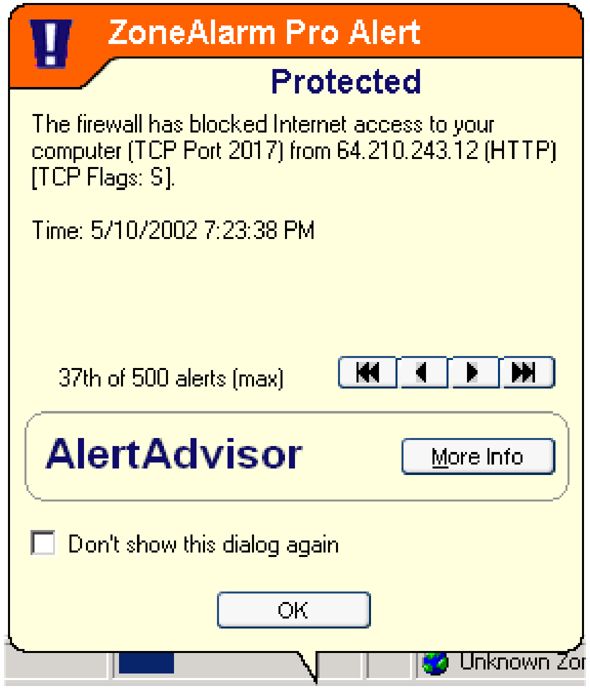
➡ 3. Firewalls, Anti-Virus

4. “Persona” details and options
5. Tracking you cyber: web browser, email, social media
6. Tracking you physical: phone, internet of things
7. Critical Advice and Summary

Online web page = http://navigators.com/issues.html

Personal Firewalls

- A firewall should monitor incoming <u>and</u> outgoing traffic
- Some firewalls are more secure than others (stateful packet inspection, ICSA Certified, etc)
- Most firewalls do not protect against viruses
- All firewalls require administration (set-up configuration, updates, granting permissions for applications)
- Change the default administrative password included in the firewall
- Event logs – learn how to read these
- You can traceroute IP addresses and search for info on port numbers



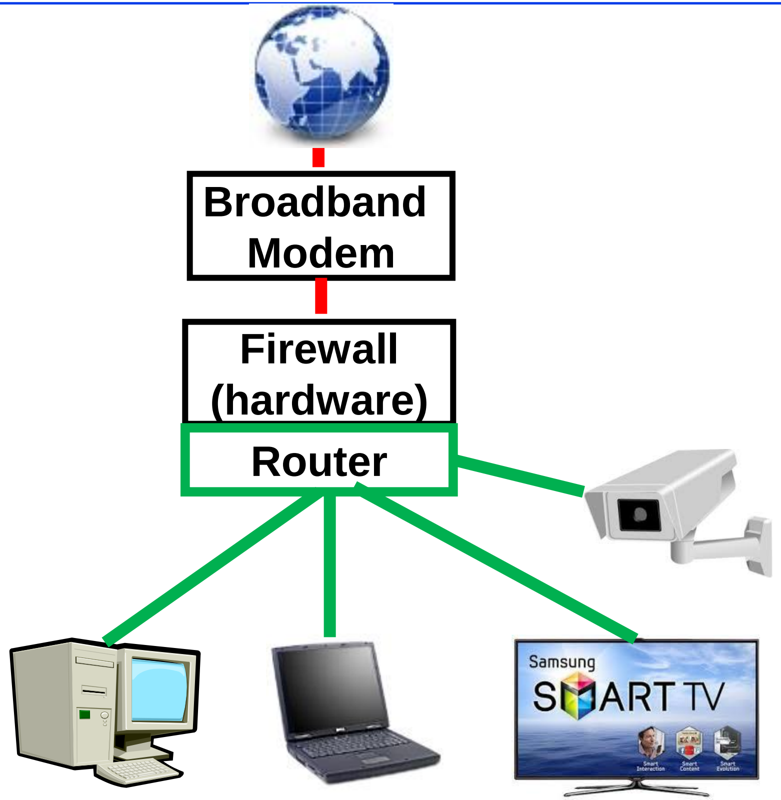
The firewall has blocked Internet access to your computer (TCP Port 2017) from 64.210.243.12 (HTTP) [TCP Flags: S].

Time: 5/10/2002 7:23:38 PM

37th of 500 alerts (max)

□ Don't show this dialog again

Firewall Options

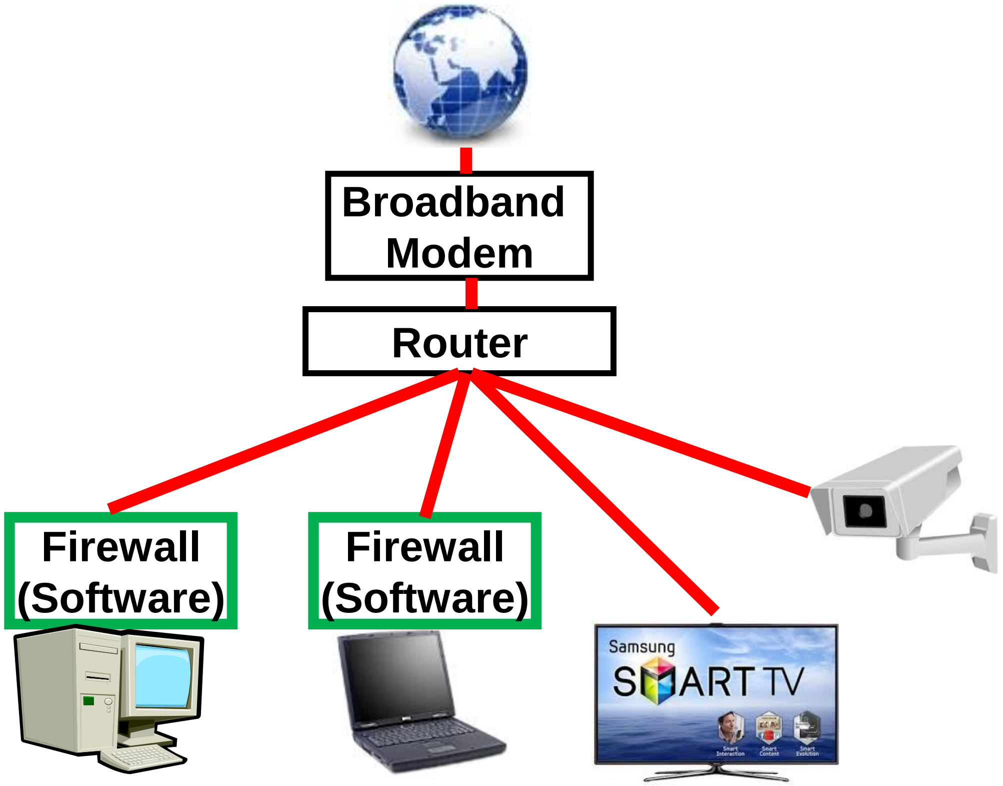


Broadband Modem

Firewall (hardware)

Router

- Cost: <$100 to ~$500
- Additional functions available
- NAT, DCHP, Email notification
- Easier for computers to locally share folders / printers
- Can protect other devices



Broadband Modem

Router

Firewall (Software)

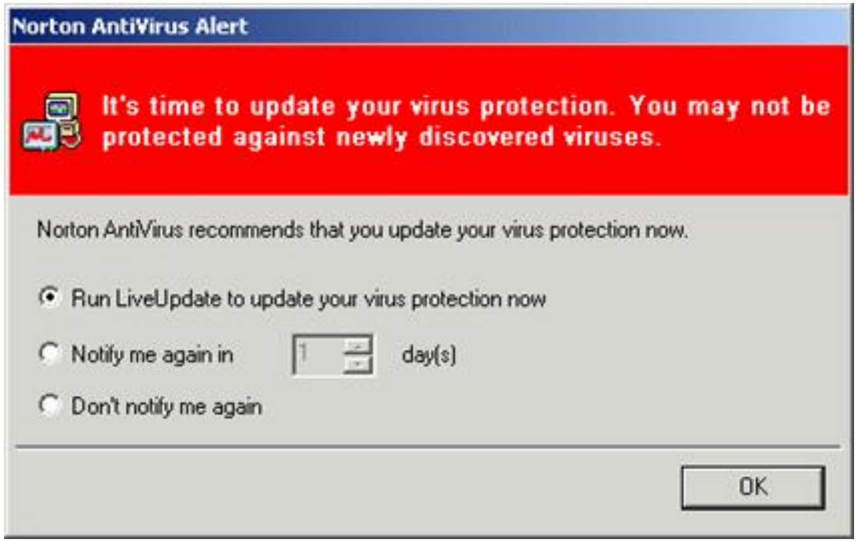
Firewall (Software)

- Cost: free to ~$50 per computer
- Each machine needs to be configured
- Firewalls may interfere with local network sharing
- What about other Internet devices?

Anti-Virus Software

- Every machine should have updated anti-virus software installed, and running
- AV software should automatically examine every incoming file (email attachment, web download, peer-to peer download)
- AV software will occasionally scan every file on your machine for viruses
- The heart of most AV programs is a “dictionary” of pre-defined viruses which is compared to your files. The dictionary may have over 1,000,000 definitions.
- AV programs will also monitor certain sensitive system resources for any changes

Important: the virus definition dictionary must to be updated frequently. There may be 100 new virus definitions added to the dictionary in one week.



Norton AntiVirus Alert

It's time to update your virus protection. You may not be protected against newly discovered viruses.

Norton AntiVirus recommends that you update your virus protection now.

● Run LiveUpdate to update your virus protection now

○ Notify me again in 1 day(s)

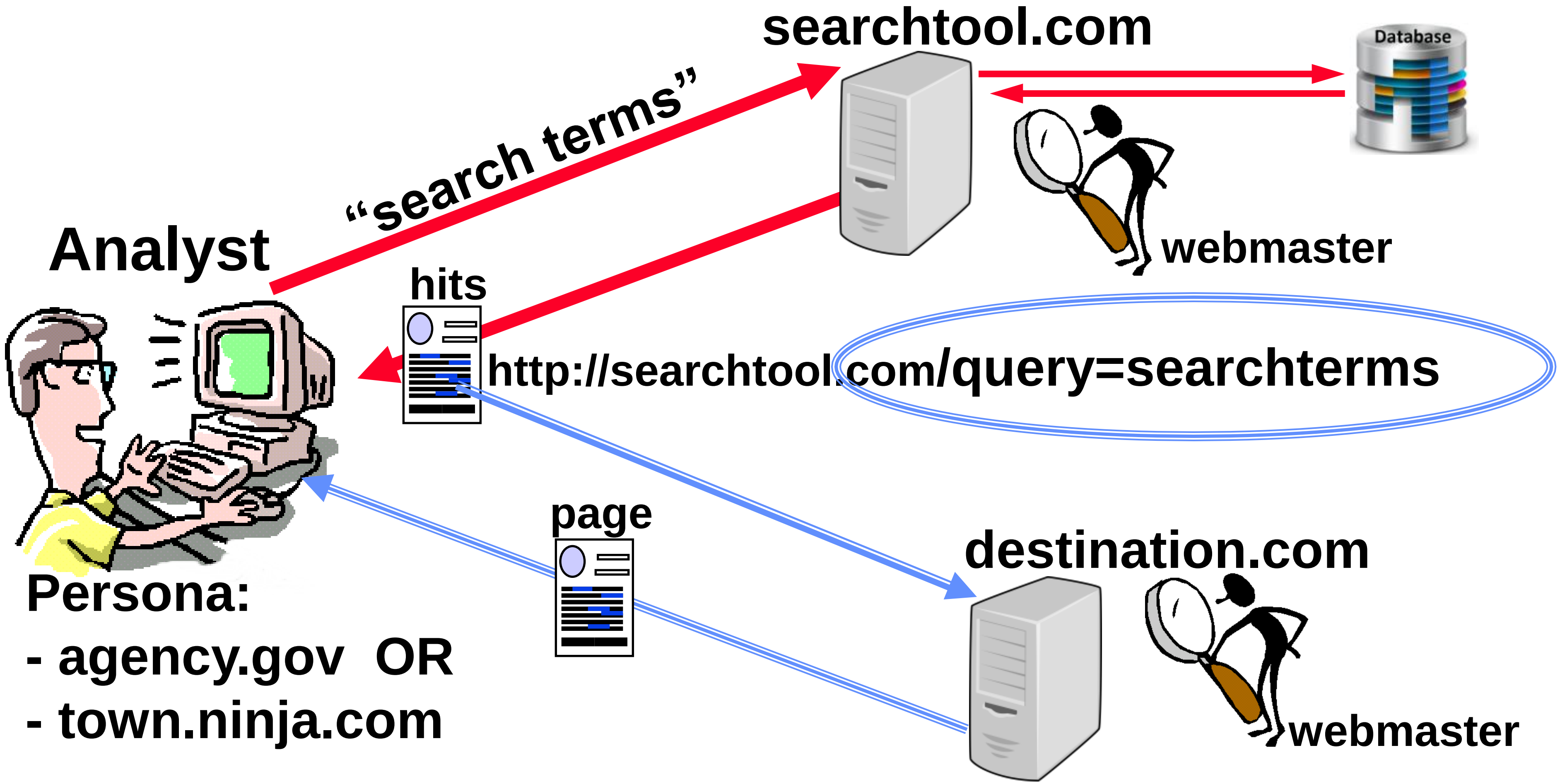
○ Don't notify me again

Security and Privacy Issues

1. Background and Statistics
2. Network connections (at work and home)
3. Firewalls, Anti-Virus
4. “Persona” details and options
5. Tracking you cyber: web browser, email, social media
6. Tracking you physical: phone, internet of things
7. Critical Advice and Summary

Online web page = http://navigators.com/issues.html

A Typical Scenario...



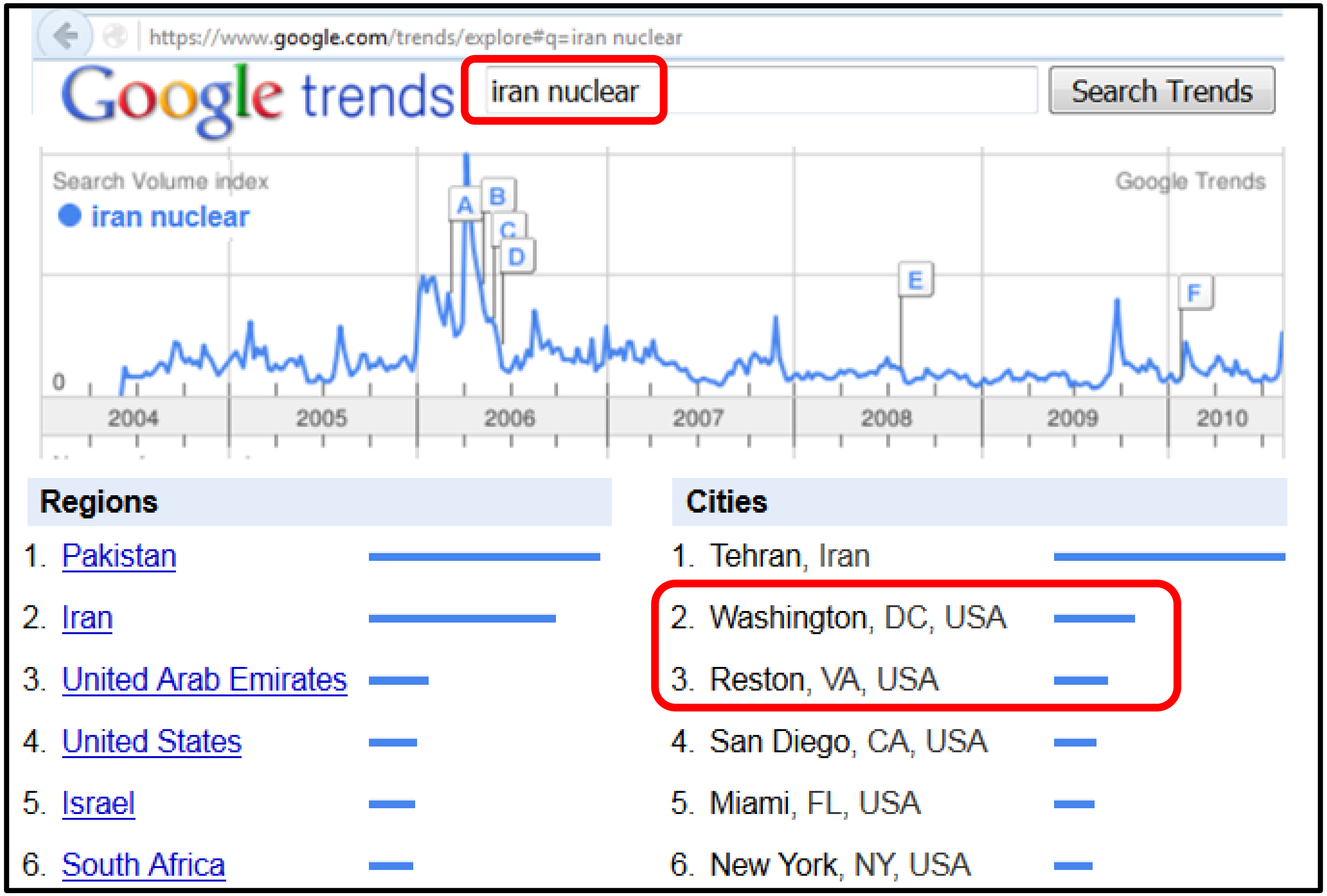
Persona:
- agency.gov OR
- town.ninja.com

━ searchtool.com webmaster knows your "search terms"

═ destination.com webmaster knows the "search terms" and search technique you used to find them

Search Tools are Tracking You

- Most search tools keep a long, detailed history of "all user activities"
- What do ALL searches from ALL your co-workers look like to a particular search tool webmaster?



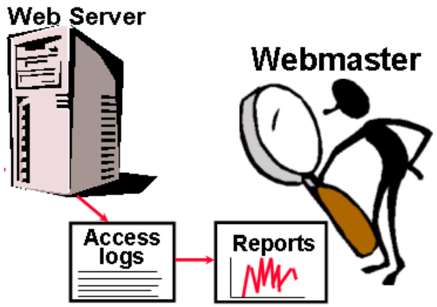
https://www.google.com/trends/explore#q=iran nuclear

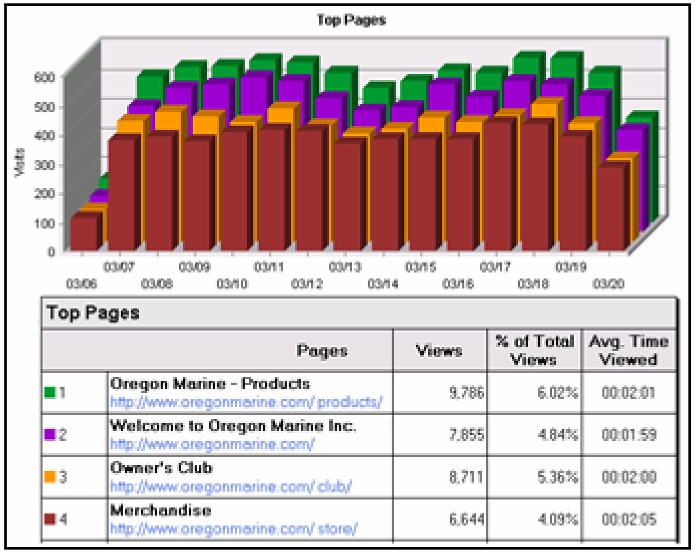
Google trends: iran nuclear

Regions	Cities
1. Pakistan	1. Tehran, Iran
2. Iran	2. Washington, DC, USA
3. United Arab Emirates	3. Reston, VA, USA
4. United States	4. San Diego, CA, USA
5. Israel	5. Miami, FL, USA
6. South Africa	6. New York, NY, USA

Web Site Log Analysis

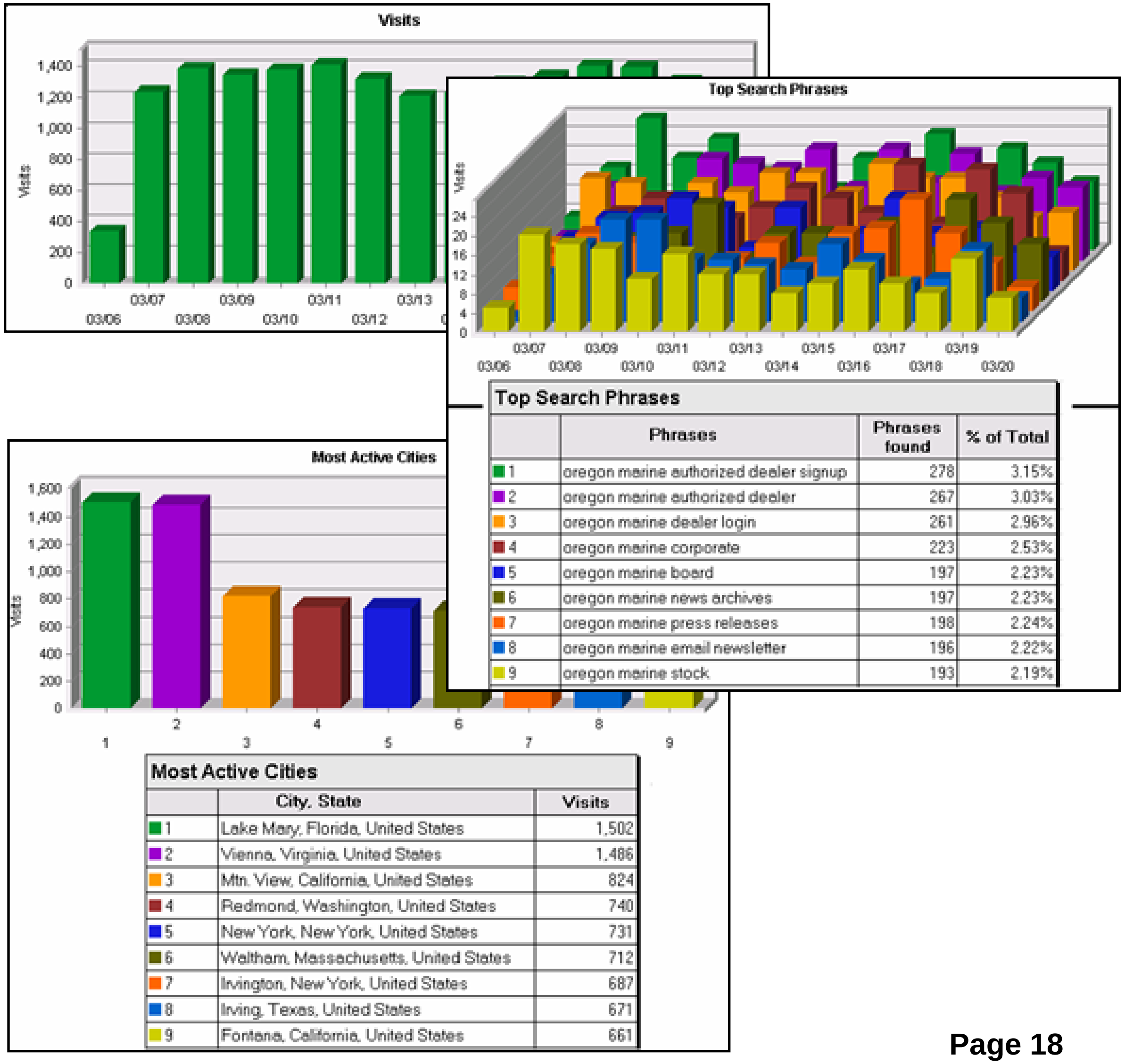
There are many standard reports that a webmaster can run





Top Pages

	Pages	Views	% of Total Views	Avg. Time Viewed
🟩 1	Oregon Marine - Products http://www.oregonmarine.com/products/	9,786	6.02%	00:02:01
🟪 2	Welcome to Oregon Marine Inc. http://www.oregonmarine.com/	7,855	4.84%	00:01:59
🟧 3	Owner's Club http://www.oregonmarine.com/club/	8,711	5.36%	00:02:00
🟥 4	Merchandise http://www.oregonmarine.com/store/	6,644	4.09%	00:02:05



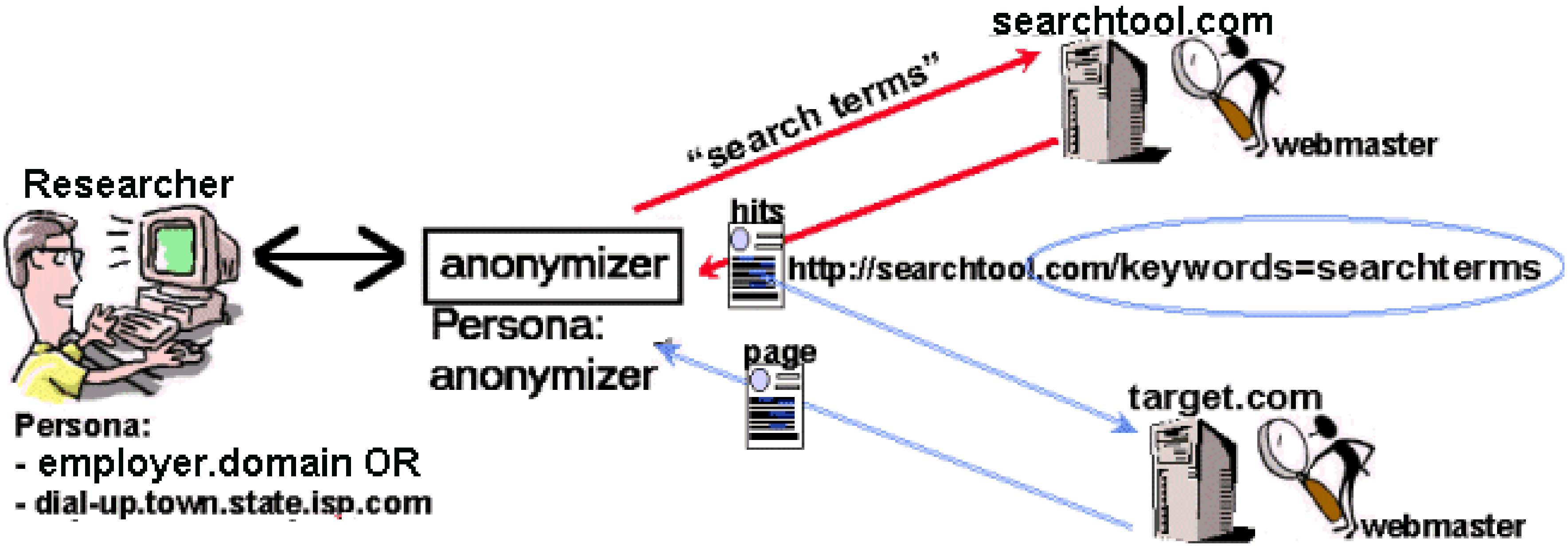
Top Search Phrases

	Phrases	Phrases found	% of Total
🟩 1	oregon marine authorized dealer signup	278	3.15%
🟪 2	oregon marine authorized dealer	267	3.03%
🟧 3	oregon marine dealer login	261	2.96%
🟥 4	oregon marine corporate	223	2.53%
🟦 5	oregon marine board	197	2.23%
🟫 6	oregon marine news archives	197	2.23%
🟧 7	oregon marine press releases	198	2.24%
🟦 8	oregon marine email newsletter	196	2.22%
🟨 9	oregon marine stock	193	2.19%

Most Active Cities

	City, State	Visits
🟩 1	Lake Mary, Florida, United States	1,502
🟪 2	Vienna, Virginia, United States	1,486
🟧 3	Mtn. View, California, United States	824
🟥 4	Redmond, Washington, United States	740
🟦 5	New York, New York, United States	731
🟫 6	Waltham, Massachusetts, United States	712
🟧 7	Irvington, New York, United States	687
🟦 8	Irving, Texas, United States	671
🟨 9	Fontana, California, United States	661

Anonymizers, VPN, Virtual platforms



- Anonymizers replace your persona with their persona
- Anonymizer now "knows your business"
- Webmasters may recognize anonymizer traffic

Anonymizer.com
Privacy is your right.

The Proxy Connection

Tor

hushmail.com !

What Kind of Persona do you have?

- Agency.gov (or branch.mil) – All web masters will easily recognize your users as members of your organization
- “non-attributable” – Do NOT use the phrase “non-attributable”. It may give the organization’s users a FALSE sense of security/invincibility, and will cause them to take excessive risks with their internet account.
  A more accurate label would be: “less recognizable”
- “less-recognizable” - This is an alternative persona/gateway which may not be “easily” associated with the organization.
  Possible concerns:
  - Many co-workers share your persona
  - Other “neighbors” of your persona
  - How frequently does the persona change (annually? monthly?)
  - Persistent Cookies, Third-party Cookies
  - Does it leak http_referrer
  - User surfing activities = the same as agency.gov users?

Internet Accounts, Policies, & Procedures

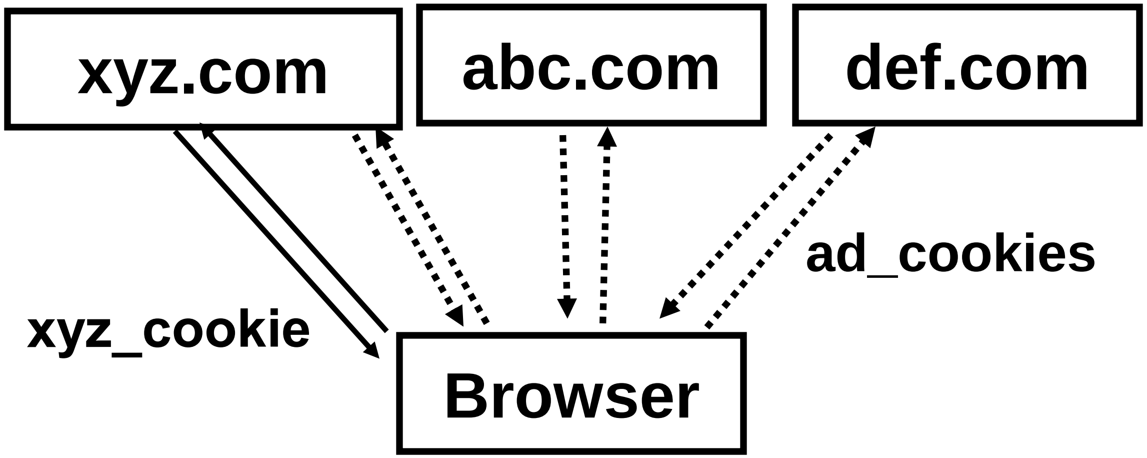
- Each type of Internet account has its own intended use, strengths and weaknesses
- Some Internet usage policies always apply
- There may also be unique policies associated with each type of account
- Policies are in a state of flux, as organizations try to keep up with the ever-changing Internet and legal environment
- Clarify these issues from within your organization
- Make sure ALL Internet users are kept aware of the latest internet usage policies. Mistakes by a handful of users could jeopardize your connection’s privacy, and cause unwanted publicity for your organization

Security and Privacy Issues

1. Background and Statistics
2. Network connections (at work and home)
3. Firewalls, Anti-Virus
4. “Persona” details and options
5. Tracking you cyber: web browser, email, social media
6. Tracking you physical: phone, internet of things
7. Critical Advice and Summary

Online web page = http://navigators.com/issues.html

Cookies


xyz.com

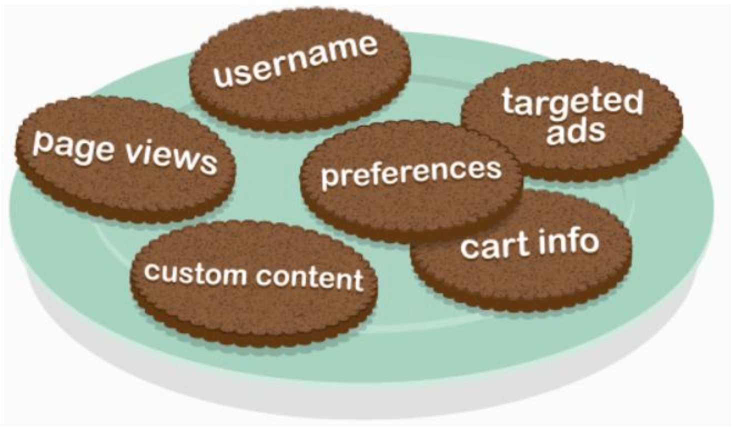
abc.com

def.com

ad_cookies

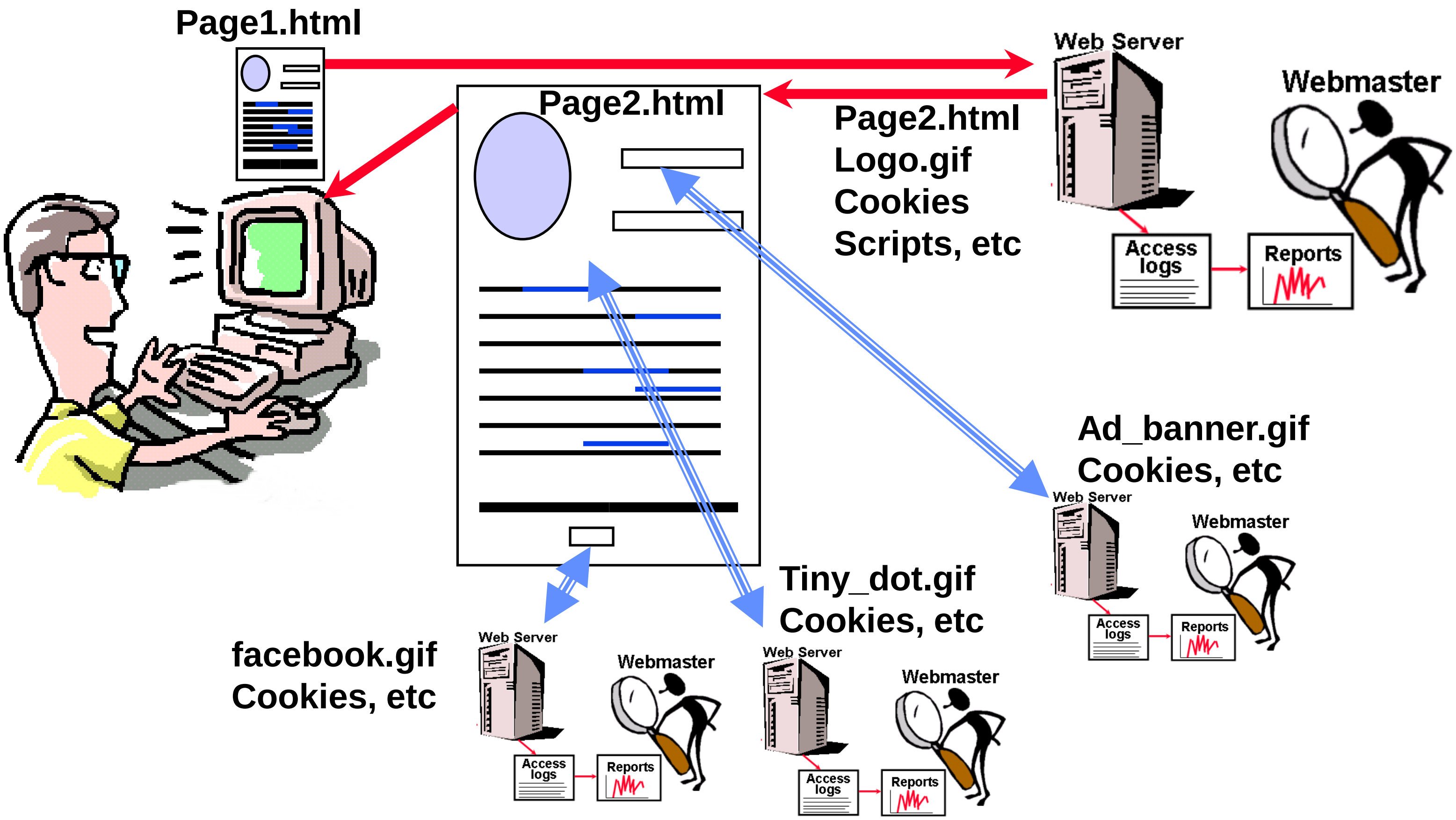
xyz_cookie

Browser



- A cookie is a piece of text stored in your computer/device
- It enables the web site to “recognize you” (username_greetings) and “remember” your interactions within the site (logged-in → shopping cart → checkout)
- Web site will repeatedly refer to your cookie and update its internal database of your online actions
- 3rd parties also place cookies on MANY web sites (advertisers, Google, Facebook, etc)

Are you visiting just one site?


Page1.html

Page2.html

Page2.html
Logo.gif
Cookies
Scripts, etc

Ad_banner.gif
Cookies, etc

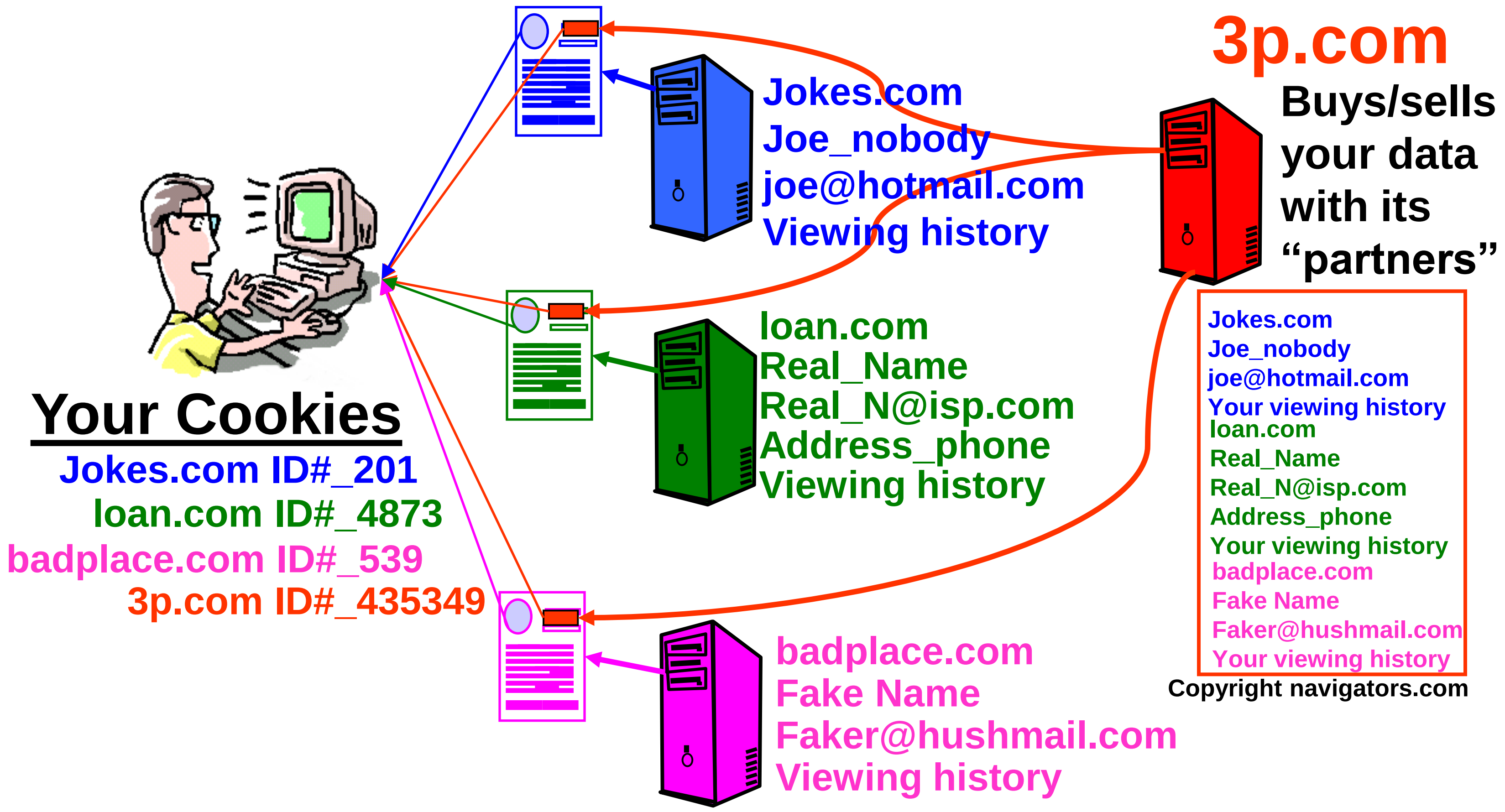
Tiny_dot.gif
Cookies, etc

facebook.gif
Cookies, etc

- Viewing a single page may cause your browser to interact with many different web servers
- Even with cookies turned off, you still make foot prints on third-party web servers while retrieving their graphics

Third Party Cookies

Most web pages include graphics/cookies/beacons from “third parties”



Jokes.com
Joe_nobody
joe@hotmail.com
Viewing history

loan.com
Real_Name
Real_N@isp.com
Address_phone
Viewing history

badplace.com
Fake Name
Faker@hushmail.com
Viewing history

3p.com
Buys/sells your data with its “partners”

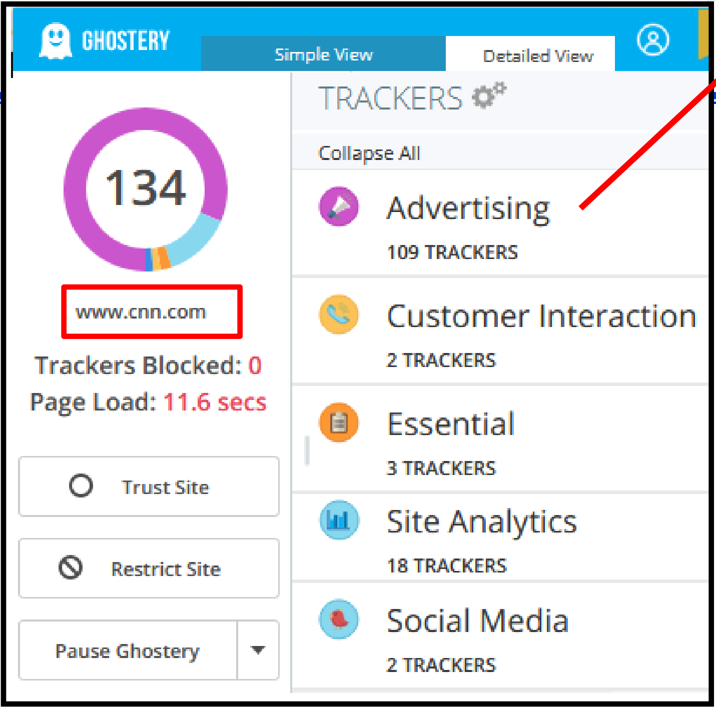
Jokes.com
Joe_nobody
joe@hotmail.com
Your viewing history
loan.com
Real_Name
Real_N@isp.com
Address_phone
Your viewing history
badplace.com
Fake Name
Faker@hushmail.com
Your viewing history

Your Cookies

Jokes.com ID#_201
loan.com ID#_4873
badplace.com ID#_539
3p.com ID#_435349

The “third party site” can compile an extensive profile on you, and sell this information to companies that are online and offline.
Google Analytics is embedded in 50% of the top 1 million websites

Trackers… https://whotracks.me



GHOSTERY

Simple View | Detailed View

134

www.cnn.com

Trackers Blocked: 0
Page Load: 11.6 secs

○ Trust Site

⊘ Restrict Site

Pause Ghostery ▾

TRACKERS

Collapse All

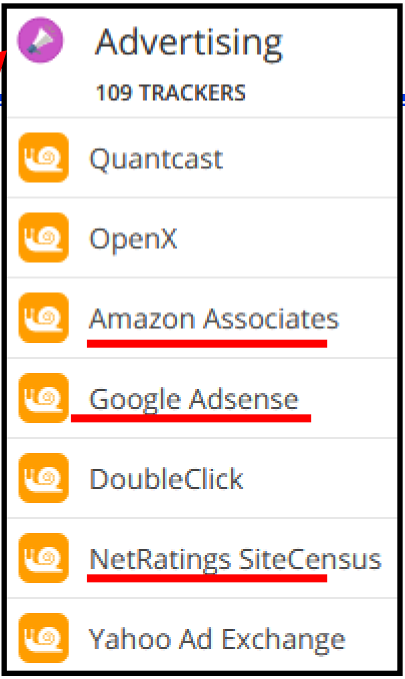
Advertising
109 TRACKERS

Customer Interaction
2 TRACKERS

Essential
3 TRACKERS

Site Analytics
18 TRACKERS

Social Media
2 TRACKERS



Advertising
109 TRACKERS

Quantcast

OpenX

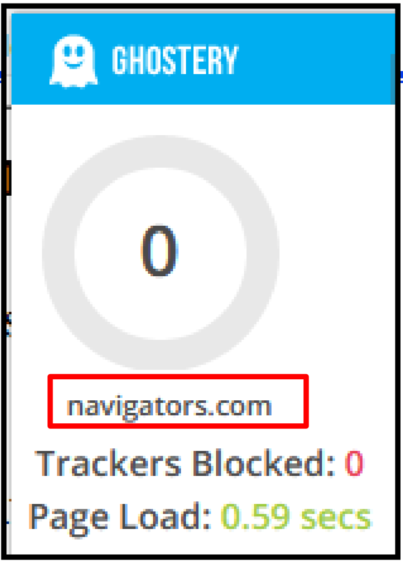
Amazon Associates

Google Adsense

DoubleClick

NetRatings SiteCensus

Yahoo Ad Exchange

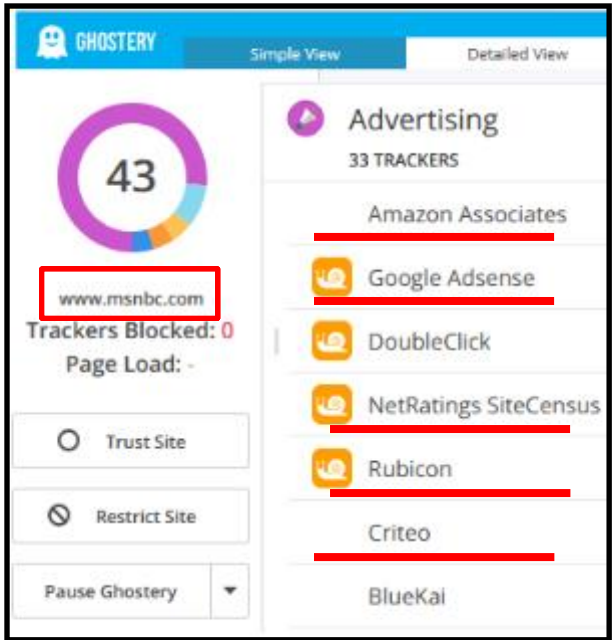


GHOSTERY

0

navigators.com

Trackers Blocked: 0
Page Load: 0.59 secs



GHOSTERY

Simple View | Detailed View

43

www.msnbc.com

Trackers Blocked: 0
Page Load: -

○ Trust Site

⊘ Restrict Site

Pause Ghostery ▾

Advertising
33 TRACKERS

Amazon Associates

Google Adsense

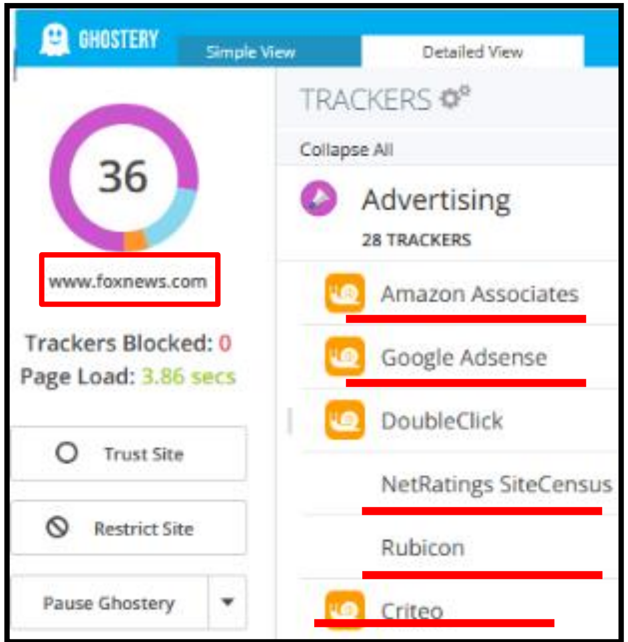
DoubleClick

NetRatings SiteCensus

Rubicon

Criteo

BlueKai



GHOSTERY

Simple View | Detailed View

36

www.foxnews.com

Trackers Blocked: 0
Page Load: 3.86 secs

○ Trust Site

⊘ Restrict Site

Pause Ghostery ▾

TRACKERS

Collapse All

Advertising
28 TRACKERS

Amazon Associates

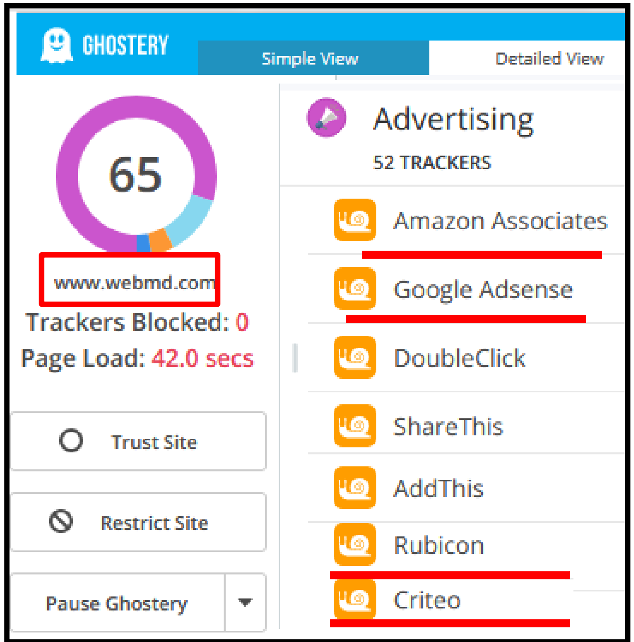
Google Adsense

DoubleClick

NetRatings SiteCensus

Rubicon

Criteo



GHOSTERY

Simple View | Detailed View

65

www.webmd.com

Trackers Blocked: 0
Page Load: 42.0 secs

○ Trust Site

⊘ Restrict Site

Pause Ghostery ▾

Advertising
52 TRACKERS

Amazon Associates

Google Adsense

DoubleClick

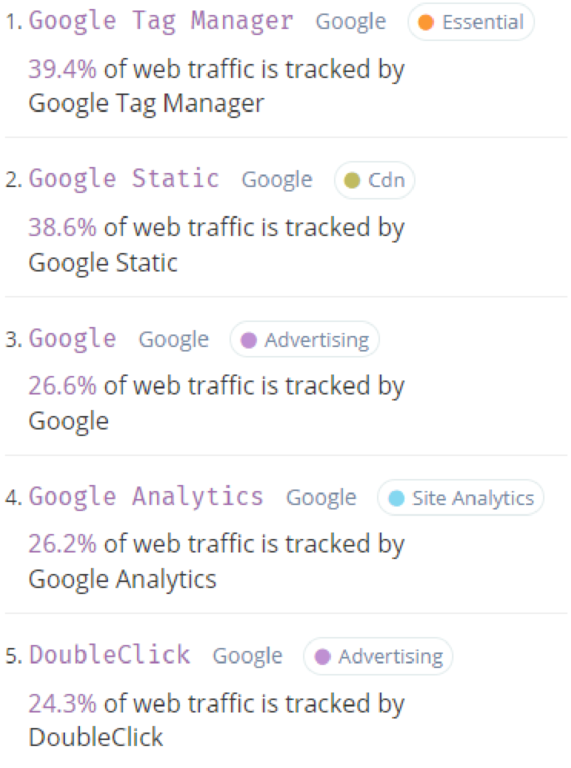
ShareThis

AddThis

Rubicon

Criteo

~850 Trackers listed at: whotracks.me



1. Google Tag Manager Google ● Essential

39.4% of web traffic is tracked by Google Tag Manager

2. Google Static Google ● Cdn

38.6% of web traffic is tracked by Google Static

3. Google Google ● Advertising

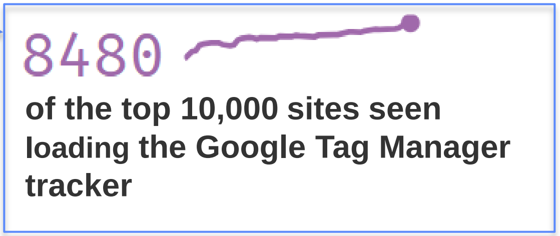
26.6% of web traffic is tracked by Google

4. Google Analytics Google ● Site Analytics

26.2% of web traffic is tracked by Google Analytics

5. DoubleClick Google ● Advertising

24.3% of web traffic is tracked by DoubleClick



8480

of the top 10,000 sites seen loading the Google Tag Manager tracker

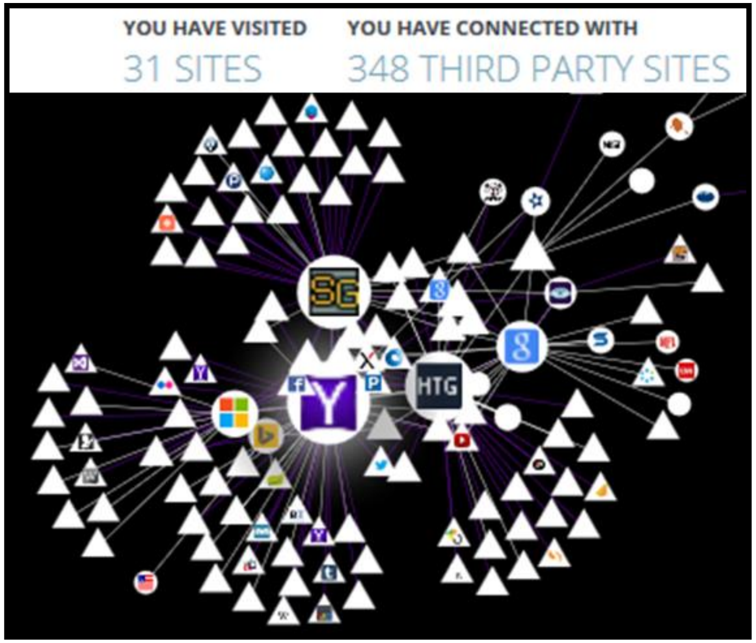
- 6. Google Fonts Google
- 7. Google APIs Google
- 8. Facebook Facebook
- 9. YouTube Google
- 10. Google User Content Google
- 11. Amazon Advertising Amazon
- 12. Amazon CloudFront Amazon
- 13. Google Syndication Google
- 14. Google Photos Google
- 15. CloudFlare Cloudflare
- 16. ScoreCard Research comScore
- 17. jsDelivr
- 18. Amazon Web Services Amazon
- 19. Twitter Twitter
- 20. Optanaon by OneTrust OneTrust
- 21. Amazon CDN Amazon
- 22. Bing Ads Microsoft
- 23. New Relic New Relic
- 24. Sentry Sentry
- 25. Criteo Criteo
- 26. Adobe Audience Manager Adobe
- 27. Quantcast Quantcast International
- 28. Yandex Metrika Yandex
- 29. OneTrust OneTrust
- 30. AppNexus AppNexus Inc.
- 31. Facebook CDN Facebook
- 32. Reddit reddit
- 33. Microsoft Services Microsoft
- 34. Hotjar Hotjar
- 35. Google AdServices Google
- 36. Taboola Taboola
- 37. ChartBeat ChartBeat
- 38. Twitter Syndication Twitter
- 39. Pinterest Pinterest
- 40. Rubicon The Rubicon Project,
- 41. Akamai Technologies Akamai
- 42. PubMatic PubMatic, Inc.
- 43. jQuery JS Foundation
- 44. unpkg
- 45. Outbrain Outbrain

Highlight = Possible foreign ownership!

Data sold to: advertisers, politicians, government bureaus, Intel agencies, any bidder?

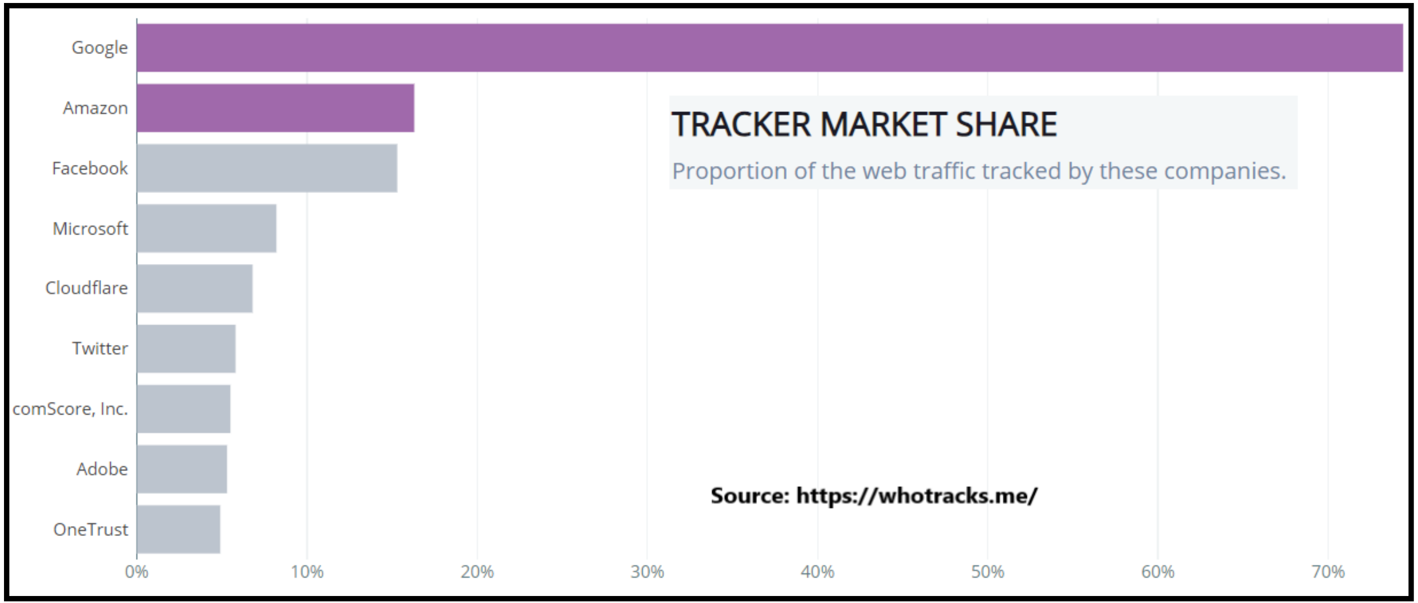
Web Bugs and Beacons

- Web bugs are “hidden” graphics
- The graphic is usually a 1 x 1 pixel and is the same color as the background
- Some web privacy policies refer to web bugs as “beacons”
- Firefox plug-ins Ghostery and Lightbeam reveal MANY beacons



YOU HAVE VISITED 31 SITES

YOU HAVE CONNECTED WITH 348 THIRD PARTY SITES



TRACKER MARKET SHARE

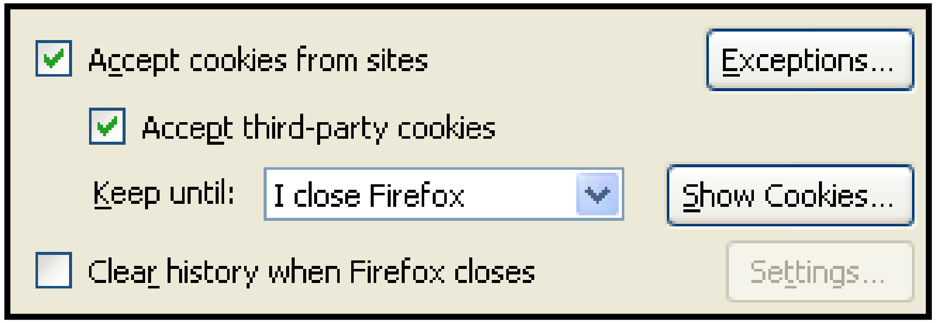
Proportion of the web traffic tracked by these companies.

Source: https://whotracks.me/

Managing Cookies

Browsers have several settings to control cookies

Tools -> Options (or Internet options)

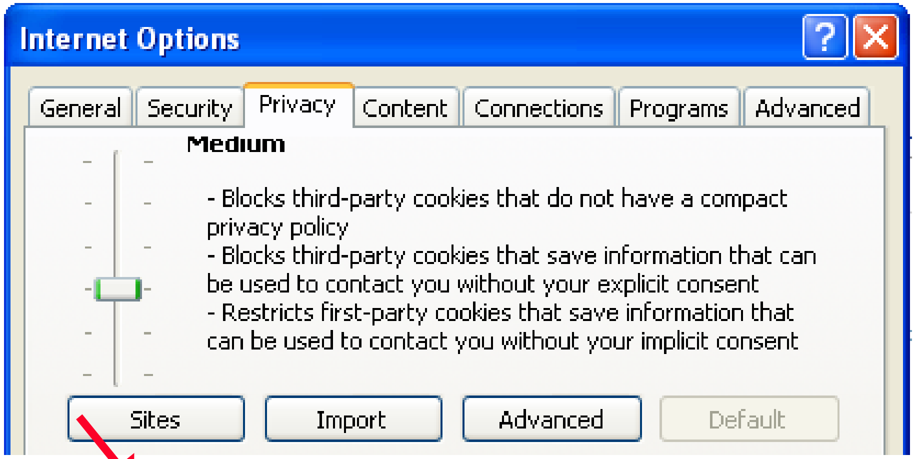


☑ Accept cookies from sites

☑ Accept third-party cookies

Keep until: I close Firefox

☐ Clear history when Firefox closes

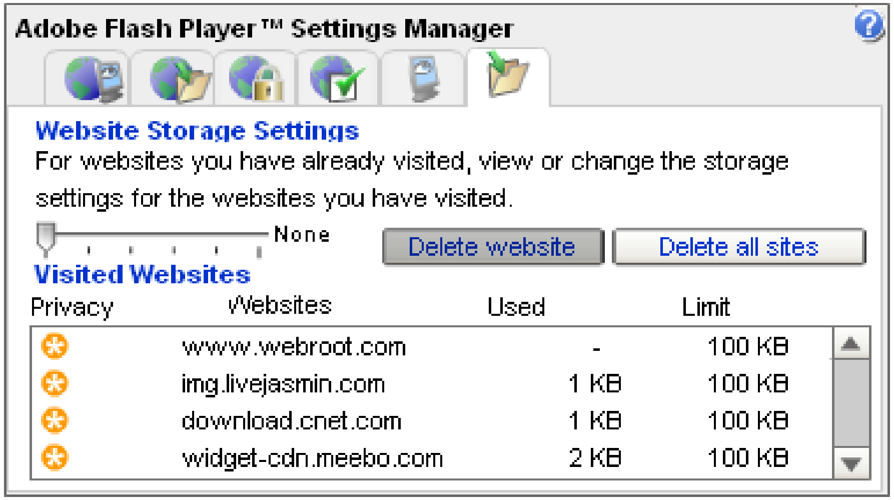


Internet Options

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

You can allow cookies from specific web sites, while blocking most other sites.



Adobe Flash Player ™ Settings Manager

Website Storage Settings

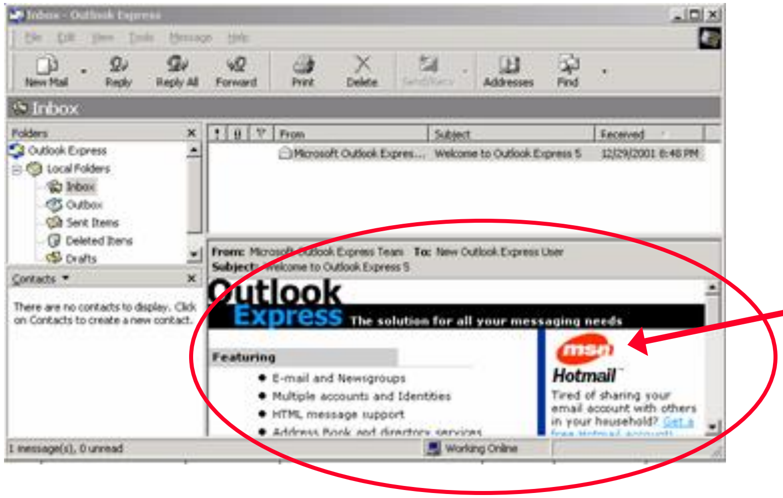
For websites you have already visited, view or change the storage settings for the websites you have visited.

Visited Websites

Privacy	Websites	Used	Limit
✱	www.webroot.com	-	100 KB
✱	img.livejasmin.com	1 KB	100 KB
✱	download.cnet.com	1 KB	100 KB
✱	widget-cdn.meebo.com	2 KB	100 KB

There are other types of trackers such as “remotely stored objects”

Reading Email = Web Surfing!



Microsoft Outlook Expres... Welcome to Outlook Express 5 12/29/2001 6:48 PM

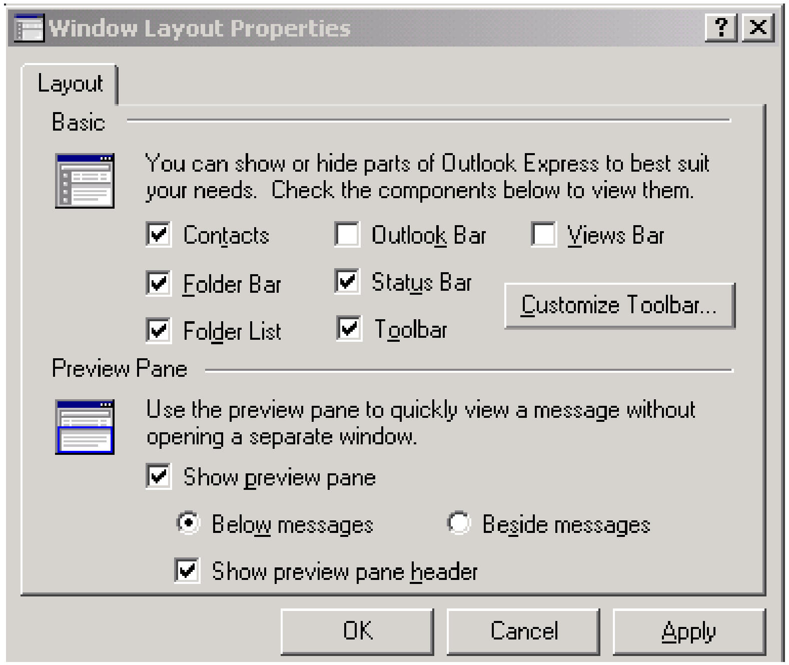
From: Microsoft Outlook Express Team To: New Outlook Express User
Subject: Welcome to Outlook Express 5

Featuring
- E-mail and Newsgroups
- Multiple accounts and Identities
- HTML message support
- Address Book and directory services

Tired of sharing your email account with others in your household? Get a free Hotmail account!

There are no contacts to display. Click on Contacts to create a new contact.

1 message(s), 0 unread



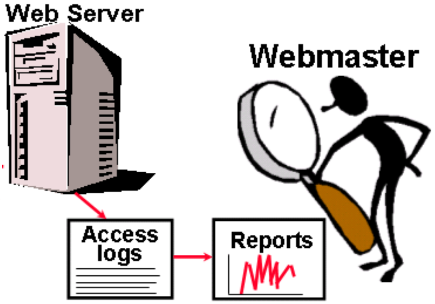
You can show or hide parts of Outlook Express to best suit your needs. Check the components below to view them.

☑ Contacts ☐ Outlook Bar ☐ Views Bar
☑ Folder Bar ☑ Status Bar
☑ Folder List ☑ Toolbar

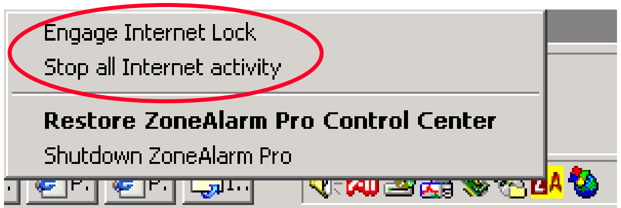
Use the preview pane to quickly view a message without opening a separate window.

☑ Show preview pane
● Below messages ○ Beside messages
☑ Show preview pane header

Graphics downloaded as you preview/display an email



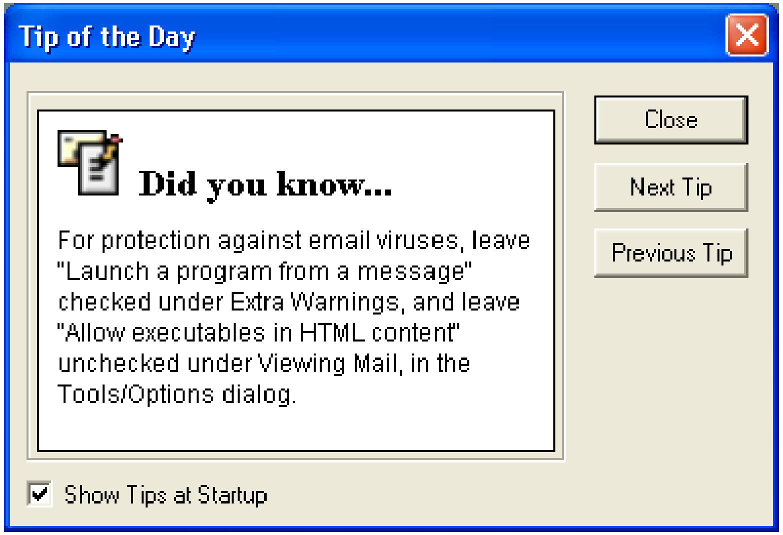
- Most graphics are downloaded from an online server as you view email
- The spammer now knows that you have read his email
- Try it yourself: www.readnotify.com
- Ways to avoid this:
  - Disable HTML, preview options
  - Block Internet while browsing downloaded email


Engage Internet Lock
Stop all Internet activity
Restore ZoneAlarm Pro Control Center
Shutdown ZoneAlarm Pro

Email issues

- Default email program settings may leave you vulnerable
- Viruses often transmitted via address books
(don’t trust any attachment – even from your friends)
- Spam – Do not reply to get “removed”
- Scams – nigeria money scam – Give us your bank account number
- Hoaxes - $300 cookie recipe, boy brain tumor, modem tax, etc.
- Social engineering – One virus hoax email told you to search for a file and delete it... Unfortunately the file in question is a normal system file

- If it says “tell everyone you know”, it IS a hoax. To confirm if it is a hoax, simply search for part of the email using google.
- Microsoft outlook – Look for updates, patches and learn about settings

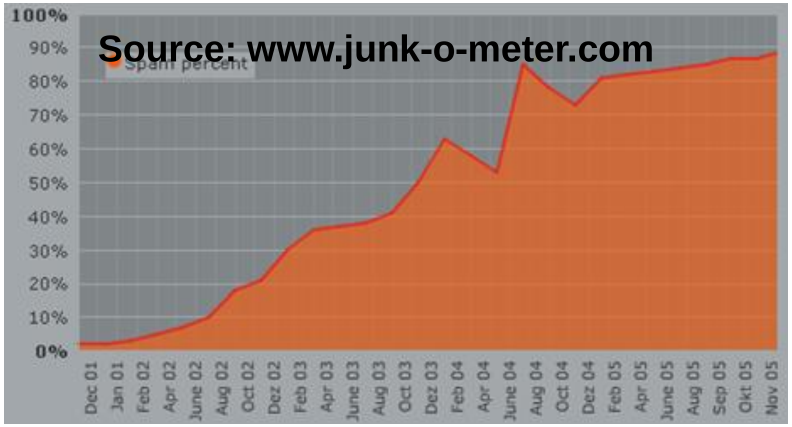


Did you know...

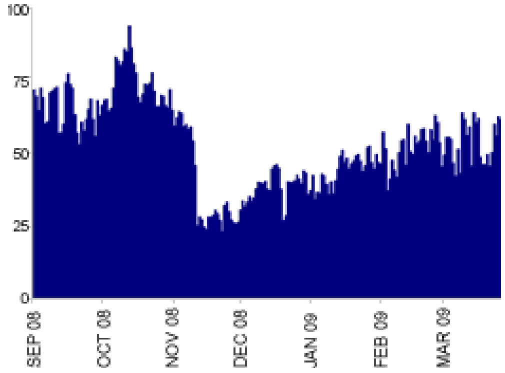
For protection against email viruses, leave "Launch a program from a message" checked under Extra Warnings, and leave "Allow executables in HTML content" unchecked under Viewing Mail, in the Tools/Options dialog.

☑ Show Tips at Startup

Spam and Phishing



Source: www.junk-o-meter.com



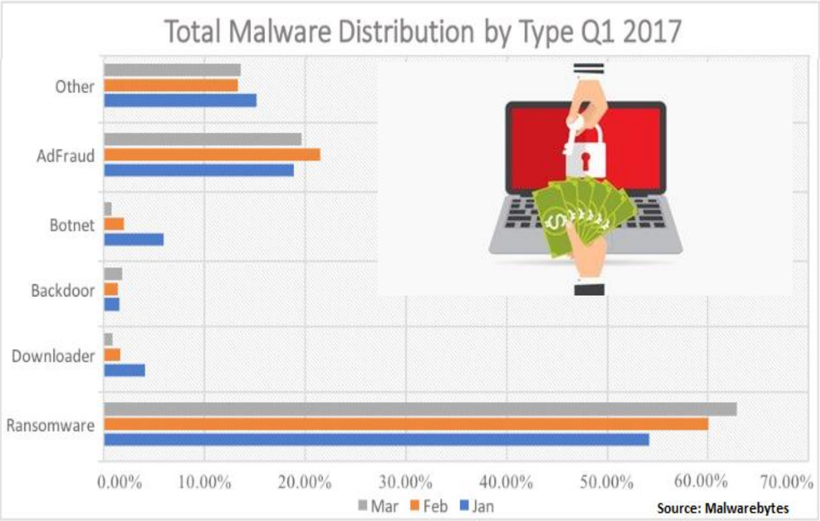
Daily Quarantined Spam Per User — *Source: Google*

- “Phishing” is sent to random users to get them infected or to reveal sensitive data
- “Spear-Phishing” is customized to you
- “Whaling” is targeted to your leadership
- Advanced Persistent Threat will target you from co-workers, family, neighbors, HOA, college alumni, child’s school, etc.

Do NOT open attachment until you contact sender using a “known”, non-email communication channel

Ransomware

- You are denied access to your data/system
- Pay… or your data is destroyed
- Ransomware has exploded in “popularity”
- Open source “kits” for anyone who wants to make some extra money
- Ransomware “as a service”
- Delivered via phishing email, social media, watering hole, compromised website



Total Malware Distribution by Type Q1 2017

Source: Malwarebytes

Your two options to cope with ransomware:

- Never click on ANY link/attachment in any email or webpage
- Have offline back-up copies of all data that you value (use a back-up program to automate the process)

Recent Malware “innovation”: crypto currency mining

Future: “Internet of Things” + ransomware = chaos!

Social media must be managed…

- Mailing lists – If you post a message to a mailing list…
  Do you know who else is on that list?
  Is there an archive of that list’s messages?
- Blogs such as Facebook – Assume that your content will be archived and shared with a very large audience
- Information you (or your kids) post can assist with identity theft: (birthdate, home town, name of high school, dog’s name, etc)
- Are your co-workers also Facebook friends? 8 of your friends have college degrees in “International Relations” and their kids go to Mclean High School…
- Facebook Privacy controls are splintered into many different sections and layers. New features are usually defaulted to “everyone”.
  You have to keep changing them to “friends only”

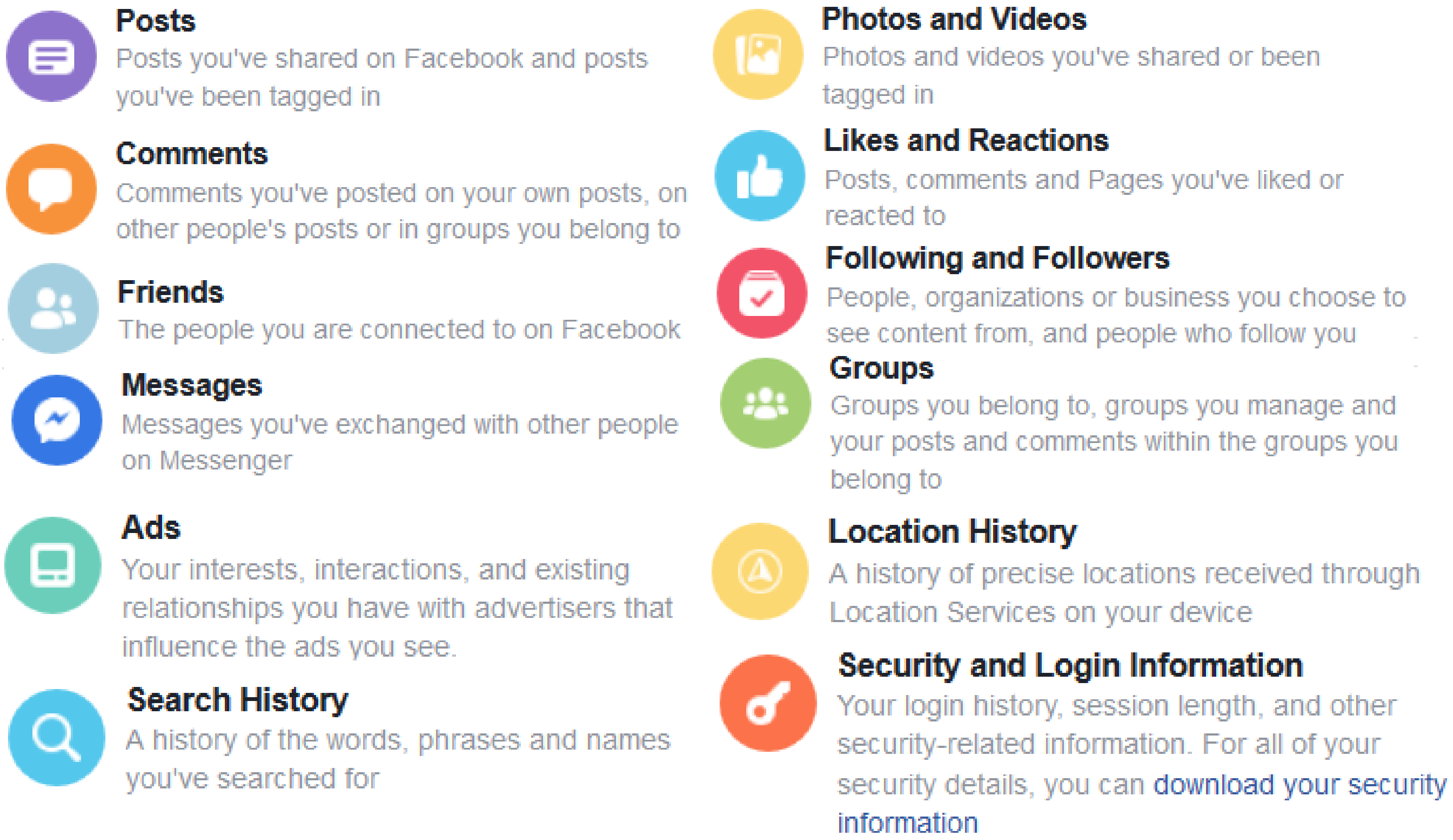
Facebook tracks you across many websites

Facebook has been “experimenting” on users

A decade of YOU on Facebook

facebook.com/settings?tab=your_facebook_information

- “Download Your Information” → “all of my data”, “HTML”
- “Access Your Information” → “expand all”



Posts
Posts you've shared on Facebook and posts you've been tagged in

Comments
Comments you've posted on your own posts, on other people's posts or in groups you belong to

Friends
The people you are connected to on Facebook

Messages
Messages you've exchanged with other people on Messenger

Ads
Your interests, interactions, and existing relationships you have with advertisers that influence the ads you see.

Search History
A history of the words, phrases and names you've searched for

Photos and Videos
Photos and videos you've shared or been tagged in

Likes and Reactions
Posts, comments and Pages you've liked or reacted to

Following and Followers
People, organizations or business you choose to see content from, and people who follow you

Groups
Groups you belong to, groups you manage and your posts and comments within the groups you belong to

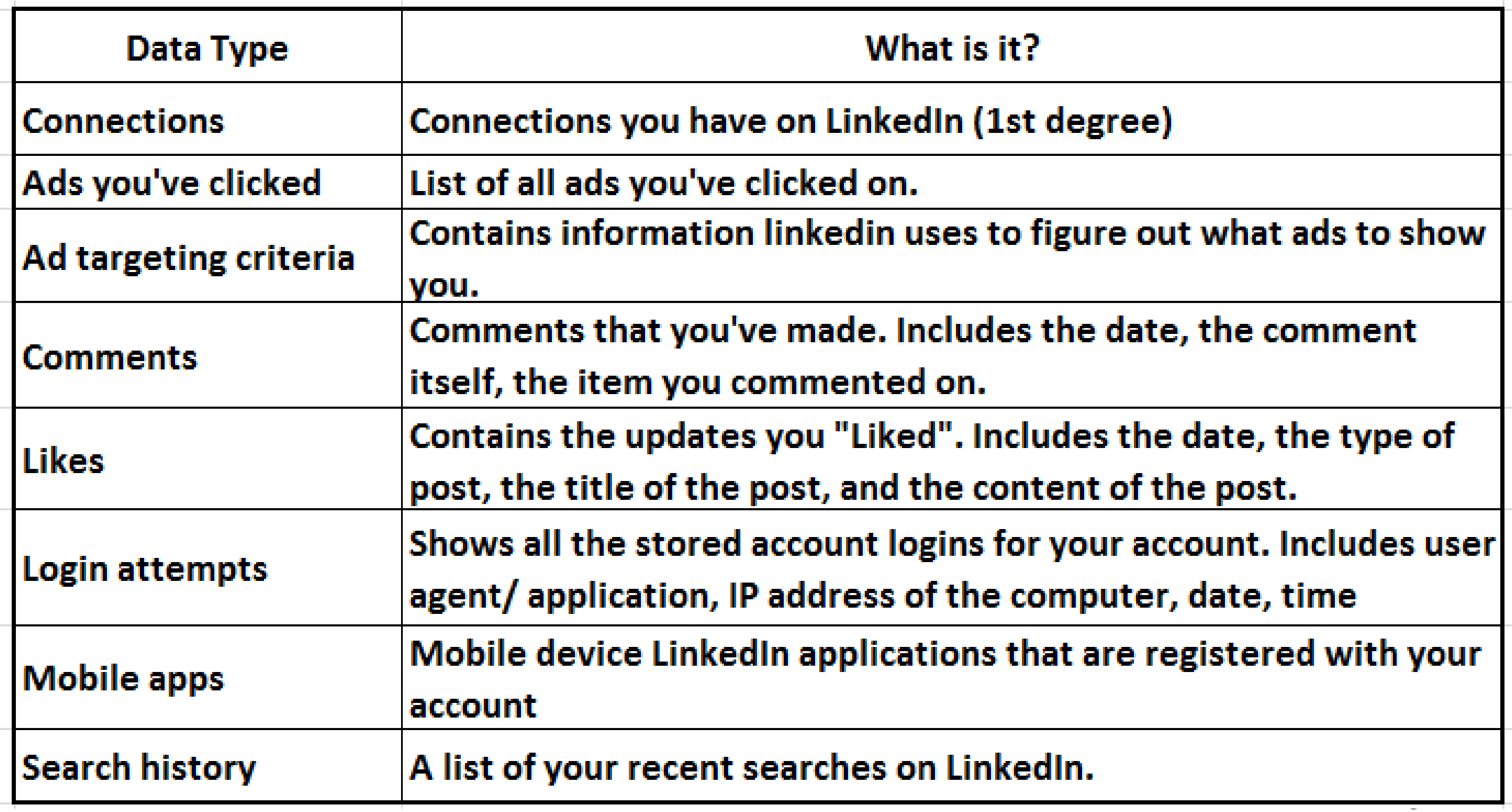
Location History
A history of precise locations received through Location Services on your device

Security and Login Information
Your login history, session length, and other security-related information. For all of your security details, you can download your security information

Download archive of Linkedin connections

linkedin.com/psettings/privacy

- “Download Your Data” → “the works”, “Request archive”
- Note: Archive comes in two separate downloads

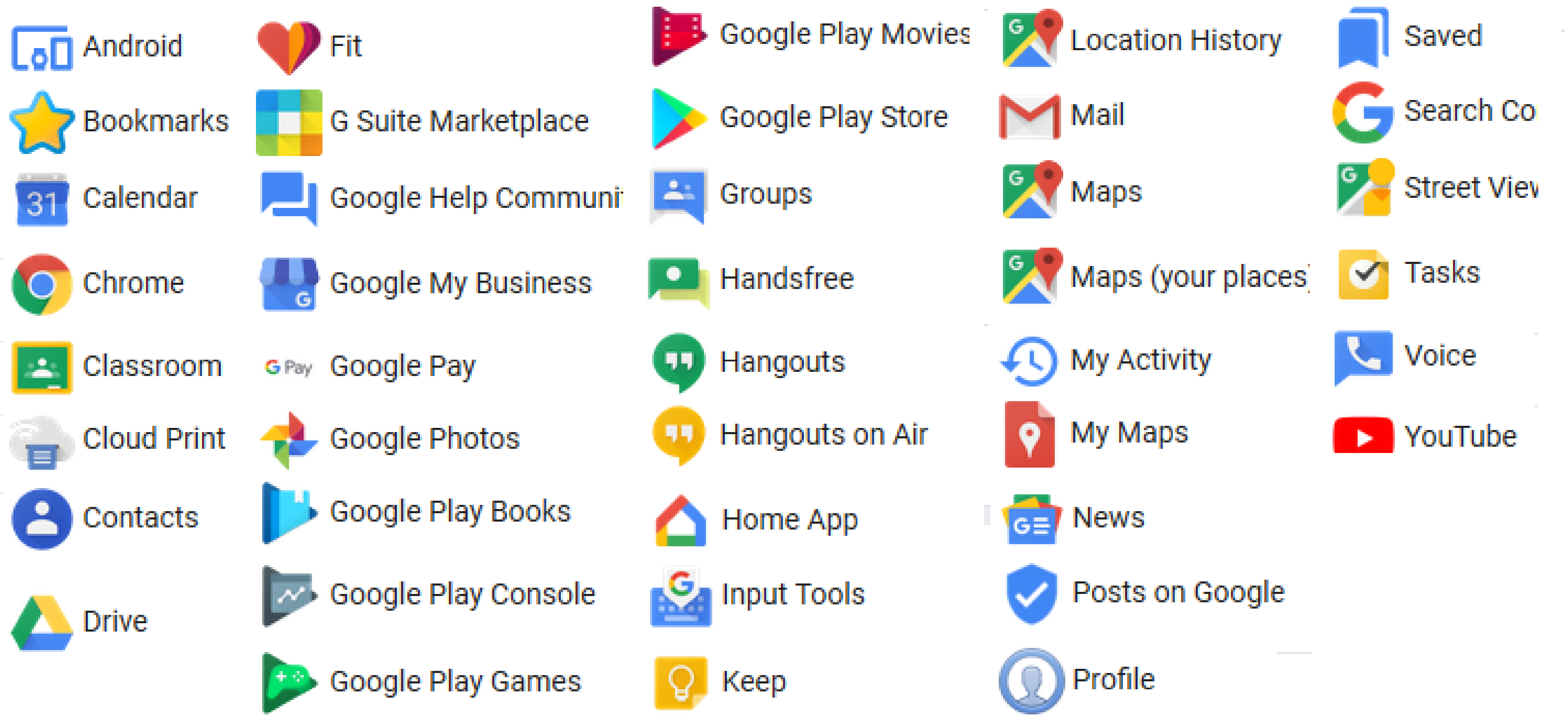


Data Type	What is it?
Connections	Connections you have on LinkedIn (1st degree)
Ads you've clicked	List of all ads you've clicked on.
Ad targeting criteria	Contains information linkedin uses to figure out what ads to show you.
Comments	Comments that you've made. Includes the date, the comment itself, the item you commented on.
Likes	Contains the updates you "Liked". Includes the date, the type of post, the title of the post, and the content of the post.
Login attempts	Shows all the stored account logins for your account. Includes user agent/ application, IP address of the computer, date, time
Mobile apps	Mobile device LinkedIn applications that are registered with your account
Search history	A list of your recent searches on LinkedIn.

Google, Gmail, YouTube, Android, etc

takeout.google.com

- Leave all selected → "next", choose file size 1GB – 50 GB



Android
Bookmarks
Calendar
Chrome
Classroom
Cloud Print
Contacts
Drive

Fit
G Suite Marketplace
Google Help Communi
Google My Business
Google Pay
Google Photos
Google Play Books
Google Play Console
Google Play Games

Google Play Movies
Google Play Store
Groups
Handsfree
Hangouts
Hangouts on Air
Home App
Input Tools
Keep

Location History
Mail
Maps
Maps (your places
My Activity
My Maps
News
Posts on Google
Profile

Saved
Search Co
Street Vie
Tasks
Voice
YouTube

Mobile Devices

- **ALL of the previous topics apply to your cell phone (persona, IP#, http_referrer, cookies, etc)**
- **AND add: microphone, camera, GPS, Wi-Fi, bluetooth, compass, accelerometer, 3-axis gyroscope, barometer**
- **Installed apps with permission, can establish a detailed pattern of life**
- **Phone can also leak to nearby smart billboards, in store tracking, car bluetooth (rental car bluetooth)**

**Any company that tracks you,
can monetize data about you**

Security and Privacy Issues

1. Background and Statistics
2. Network connections (at work and home)
3. Firewalls, Anti-Virus
4. “Persona” details and options
5. Tracking you cyber: web browser, email, social media
6. Tracking you physical: phone, internet of things
7. Critical Advice and Summary

Online web page = http://navigators.com/issues.html

Consider Alternatives

- Research “ecosystems” of products
  (Microsoft vs. Apple vs. Google)
- Alternative products may be more secure, or less targeted by hackers.
  - Browsers

  - Email Clients

  - Operating Systems

- Search before you buy: model # security breach

User Agreements... READ THEM!

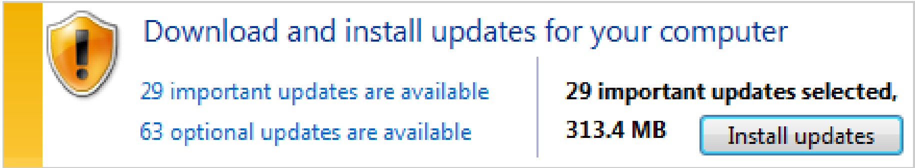
- Read user agreements for <u>everything</u> with Internet access
- Samsung Smart TV with Voice recognition:

"Please be aware that if your spoken words include
personal or other sensitive information,
that information will be among the data
captured and transmitted to a third party
through your use of Voice Recognition."

- How many microphones are in your house?
  Cell phone, tablet, laptop, flat screen TV,
  remote control (Roku, Xfinity/Comcast),
  Alexa, XBOX, Barbie doll,
  baby monitor, security camera,
  NEST thermostat

If it connects to the Internet, it must be updated

→ **All Programs → Windows Update**



Download and install updates for your computer

29 important updates are available

63 optional updates are available

29 important updates selected,

313.4 MB

- **Network devices – modem (yours or ISP’s)**
- **Router updates. Printer, network attached storage.**
- **Laptops: Windows 10, 11 Mac OS**
- **Microsoft Office**
- **Browser (Firefox, Chrome) plug-ins, Java, Flash, PDF Acrobat**
- **Other software: security suite, skype**
- **Tablet / Cell phone : Android, Apple IOS, apps**
- **“Internet of Things” - Xbox, Wii, playstation, DVR , Roku, Smart TV, blu-ray/dvd player, stereo, alarm system, fitness devices, cameras, smart watch, home automation – thermostat, switches, refrig, car, kid’s toys**

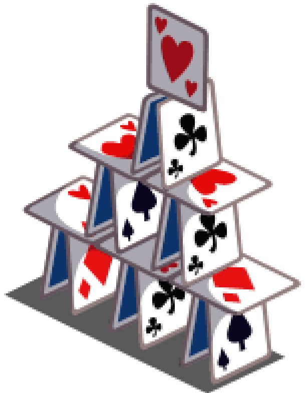
Password Chaos

- Current plan: A handful of simple passwords persistently re-used on 30+ accounts!
- Complex password = 12+ LeTtErS, numbers, characters
- If writing it down, portions of password should be camouflaged
- Example: Go = Go out and play in the back yard = Goapitby
  Write: Go98(* → type: Goapitby98(*
  Its = It's the end of the world as we know it = Iteotwawki
- 30 accounts need 30 different passwords (sounds complicated)
- Customize your password for each account
- Example: Amazon begins with "Am", Netflix begins with "Ne"
  Write: Amazon = GoAm98(* → type: GoapitbyAm98(*
  Write: Netflix = GoNe98(* → type: GoapitbyNe98(*
  Write: Citibank = ItsCi3# → type: IteotwawkiCi3#

Resetting Your Password

- Hacker can't guess your password… They click on "forgot password"
- At the target website:
  - Password hints… based on public information?
  - Extra questions to verify identity … Also based on public information?
- Via email reset..
  - Send password reset link to your email
  - Hacker breaks into your email… they can discover all other accounts that send you email (banking, shopping, etc)
  - Your email account = keys to how many other accounts?
- Two factor authentication? – "something you know" + "something you have"
- A confirmation text or reset code sent to your cell phone:
  - Your cell phone = keys to how many other accounts?

Your email and cell phone =
gateway to ALL your other accounts



Beware of Infrastructure in Public Places

- Public Computers in Library, Hotel Lobby, etc
- Is there any kind of consistent “administration” to guarantee the integrity of these computers?
- For a public computer, always assume that the machine has been compromised, and that a “keystroke logger” is quietly capturing all keystrokes
- Public Wi-Fi (hotel, Starbucks, etc)
  – packet sniffer can capture all traffic
- Ignore all software update notices while on public Wi-Fi
- Use a VPN Service
- USB charger port at airport / hotel – Use your own USB adapter and plug directly into electrical outlet
- Never use a free or “found” thumbdrive

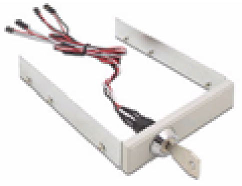
Consider Offline Storage

$400+ : A second PC without a network connection. You can use a KVM switch to run this PC to your existing keyboard/monitor

$350 : an extra notebook computer

Where will you store the offline media?

~$100 : Second hard disk – can be external, or internal with a lock key to switch disks



Removable media – optical or magnetic storage

USB flash drive – some include encryption

Local Set-up options

- Consider using encryption at home to protect personal data . For example, encrypted file systems are now standard in Windows.
- Some applications offer encryption schemes for files (quicken), but these are not very secure. There are numerous “cracker” programs which will easily break these open.
- Require passwords for access to computers or internet access
- Create multiple user accounts (even for yourself)
- Physical security of computer

Worst case considerations

- Look at the content of your hard drive - what if a clever website were able to copy your files?
- What if ransomware were to lock-up/destroy your files?
- If your research requires you to visit “exotic places” you should use a “sacrificial machine” - which has a very “bland identity”
- On the “sacrificial machine”, never use personalized sites (Gmail, amazon, local restaurant, etc)

Future

- Biometric scanner – finger, face recognition, voice, eye
- Other devices leaking information –cell phone/ Car, IOT
- Much personal Information is in databases: phone number, map, county taxes, DMV, court records, supermarket purchases, credit card company, phone company records, etc.
- Proposed law would give copyright owners the right to hack your PC
- Patent filed by Verizon to use microphone and cameras in your house to customize ads sent to your TV/phone/tablet

Fingerprint scanner as USB accessory
or built into a notebook

Exercise: Count your digital connections…

How many	Devices at Home
	cell phones
	tablets
	computers/laptops
	Gaming Systems (Xbox, PlayStation)
	smart TV
	streaming (ROKU, Amazon Fire)
	TV remotes with microphone
	Router, Modem, Printer
	Alexa /Siri / Google home video doorbell
	smart plugs/lights/appliances
	fitness tracker/Peloton
	baby monitor, Nanit, findmykids
	Car with links to online & your devices / fast pass
	Navigation, google map apps
	ALL other WIFI enabled devices:
	Roomba, smart oven, thermostat
	VOIP (skype, signal, google)

How many	Online accounts
	Email
	gmail / yahoo-mail / outlook.com / apple
	Hotmail, AOL mail
	employer.com
	client.gov
	client.internal
	Social Media
	Facebook, messenger Instagram, TikTok
	LinkedIn, signal
	snapchat, twitter
	reddit Pinterest
	gambling: DraftKings, fanduel
	photo albums, flikr
	productivity
	google docs, calendar
	OneDrive , dropbox
	Medical
	mychart, goodRX
	UnitedHealthcare
	followmy health

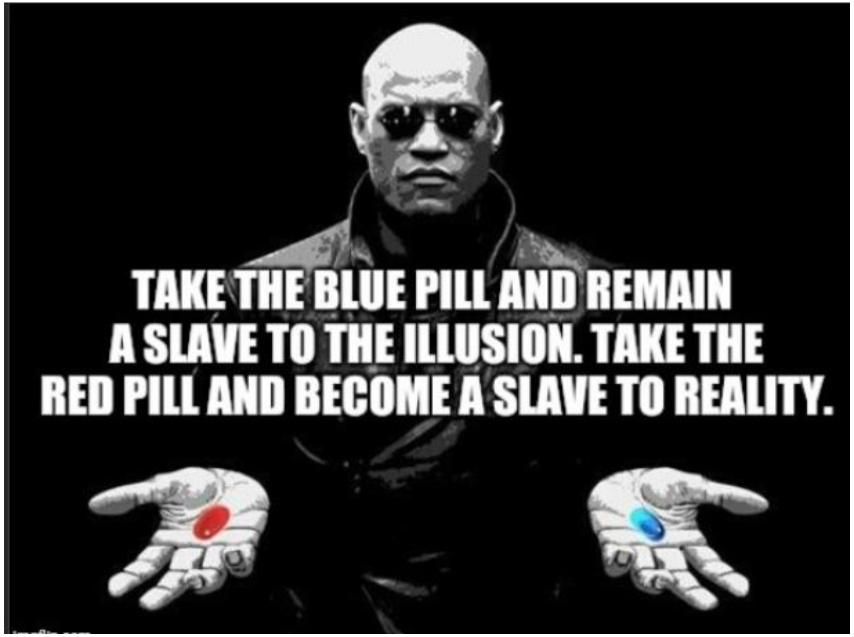
How many	Online Commerce
	Stores
	amazon /Pinterest/eBay
	Walmart / target/ home depot
	Food
	doordash, uber eats, grubhub
	open table, untapped, dominos
	Travel
	ride sharing - uber, lyft
	Frequent traveler member at: airline, hotels, rental car
	Airbnb, VRBO, booking.com
	Ticketmaster, stubhub, fandango
	Online Payment
	PayPal, Zelle, Venmo, apple pay
	Cryptocurrency bitcoin /Ethereum
	Credit cards

The Matrix has you!

Advertisers are some of the best technical targeters out there because they can see:

- what a person is doing,
- where they are doing it,
- how effective their work has been to date!

See how deep the rabbit-hole goes


TAKE THE BLUE PILL AND REMAIN A SLAVE TO THE ILLUSION. TAKE THE RED PILL AND BECOME A SLAVE TO REALITY.

NETFLIX
The Social Dilemma

<u>You</u> as a targete~~r~~!

- Advertisers <u>are</u> focused on YOU!
- Adversary Targeter focused on YOU?
- Many targeting concepts can be illustrated by understanding the personal digital environment (selectors, devices, network)
- The "IAPM Guide" has great details
- Shows how much user data is collected,
  leaked / shared / sold by default
- If someone has implemented <u>many</u> of these tips, does that indicate they have security/OPSEC training?

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS

TWELFTH EDITION, MARCH 2021

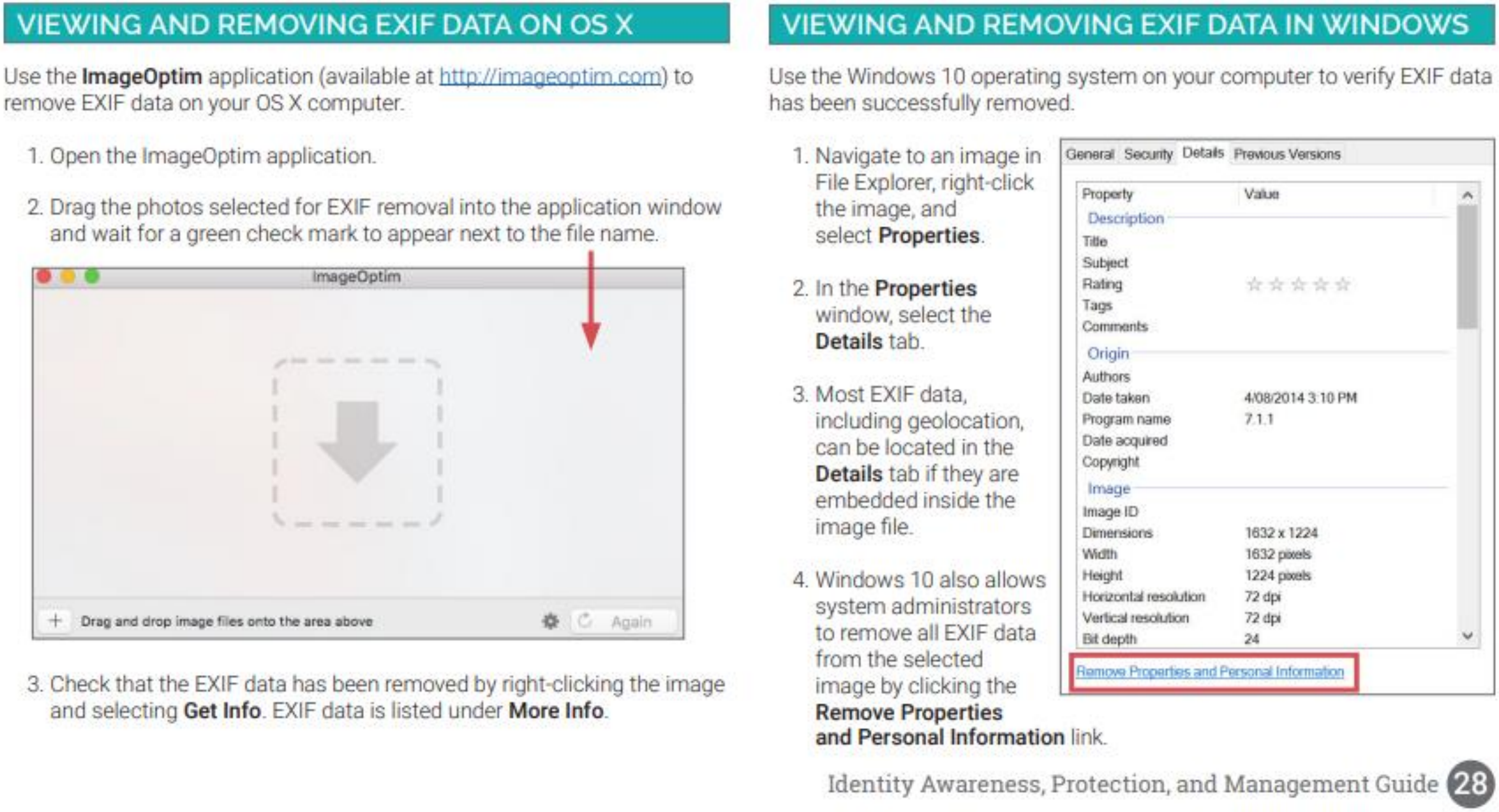
BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

www.odni.gov/files/NCSC/documents/campaign/DoD_IAPM_Guide_March_2021.pdf

Location details (EXIF) in your photos

---> Additional Details in IAPM Guide: Pages 25-28



VIEWING AND REMOVING EXIF DATA ON OS X

Use the **ImageOptim** application (available at http://imageoptim.com) to remove EXIF data on your OS X computer.

1. Open the ImageOptim application.
2. Drag the photos selected for EXIF removal into the application window and wait for a green check mark to appear next to the file name.

ImageOptim
+ Drag and drop image files onto the area above
Again

3. Check that the EXIF data has been removed by right-clicking the image and selecting **Get Info**. EXIF data is listed under **More Info**.

VIEWING AND REMOVING EXIF DATA IN WINDOWS

Use the Windows 10 operating system on your computer to verify EXIF data has been successfully removed.

1. Navigate to an image in File Explorer, right-click the image, and select **Properties**.
2. In the **Properties** window, select the **Details** tab.
3. Most EXIF data, including geolocation, can be located in the **Details** tab if they are embedded inside the image file.
4. Windows 10 also allows system administrators to remove all EXIF data from the selected image by clicking the **Remove Properties and Personal Information** link.

Property	Value
Description	
Title	
Subject	
Rating	☆ ☆ ☆ ☆ ☆
Tags	
Comments	
Origin	
Authors	
Date taken	4/08/2014 3:10 PM
Program name	7.1.1
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	1632 x 1224
Width	1632 pixels
Height	1224 pixels
Horizontal resolution	72 dpi
Vertical resolution	72 dpi
Bit depth	24

Remove Properties and Personal Information

Identity Awareness, Protection, and Management Guide 28

Final Advice

- Always be self-aware of your persona
- Know what policies apply to you
- Go HOME – make backups (just in case)
- Update all software from
  modem → smart watch
- Download a copy of: "your Facebook data",
  "what Google knows about you",
  "Linkedin profile"
- Email & social media = THE attack path to you!!
- Confirm the sender before you click on anything
- www.odni.gov/files/NCSC/documents/
  campaign/DoD_IAPM_Guide_March_2021.pdf

Summary

- ALL Internet accounts make footprints
- Online companies are finding new ways to monetize YOU
- A determined attacker can take the time to research YOU, and create the “perfect” PHISH bait
- Ensure ALL Internet users know the best tradecraft techniques to minimize devastating leaks to targets / public

Master the Information Superhighway
or
Become Roadkill

Ouch, I should have used OPSEC & Tradecraft