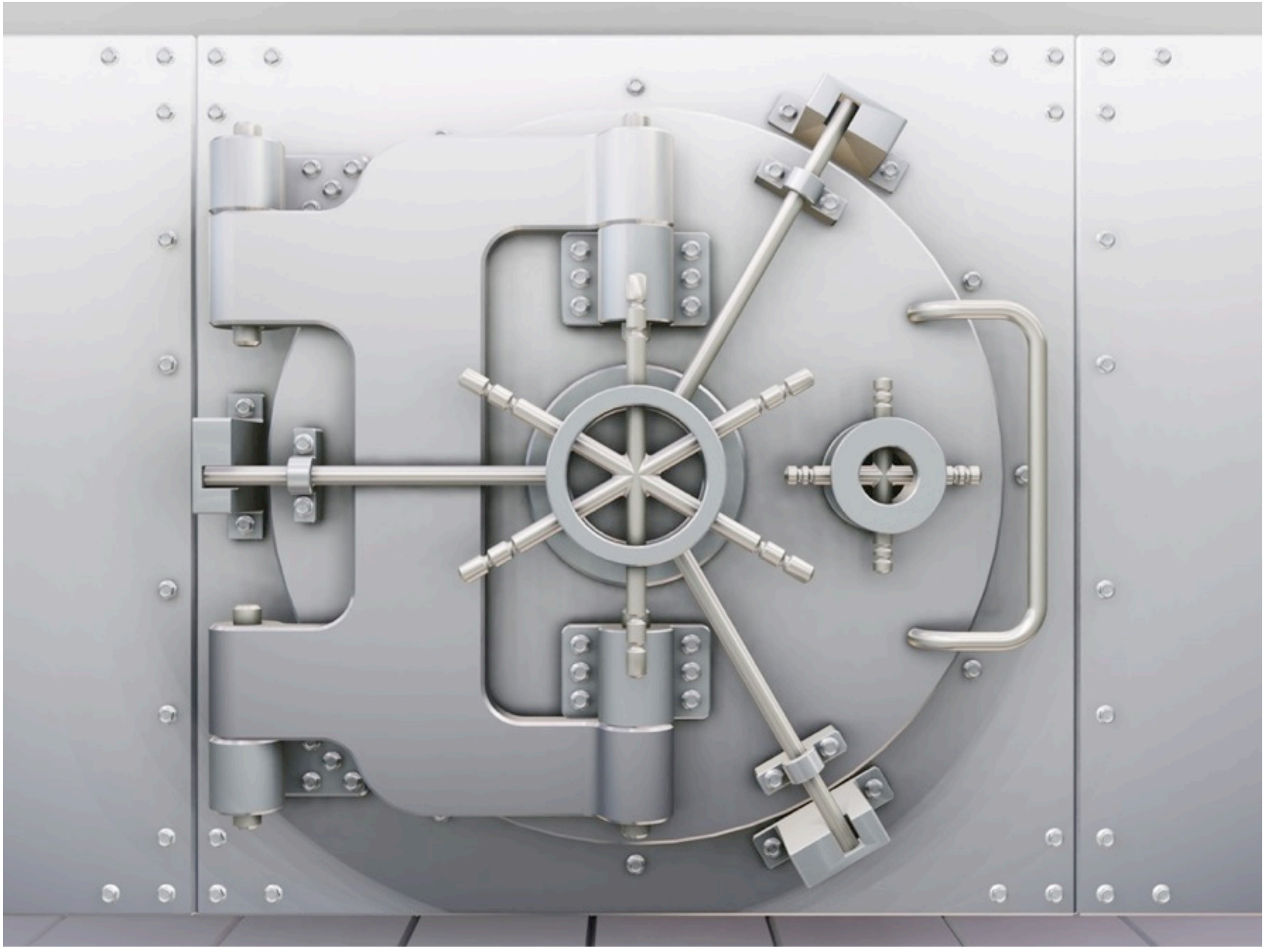
Malware:
No One Is Safe

Rik Farrow © 2012
rikfarrow.com



Typical Level of Computer Security

Aren't Macs Secure?

- Flashback infected over 600,000 Macs
  - April 2012
- OSX/Sabpab-A is a backdoor Trojan
  - April 2012
- MacControl Trojan uses Word Documents
  - March 2012

What's Changed?

- Macs have become popular
- In the 1990s, 10% of all viruses were for Macs
  - 10% of all home computers were Macs
- As Macs have become more popular, they have become attack targets

Blame Alan Turing

- Alan Turing created the notion of a Logical Computing Machine: a Turing machine
  - All of today's computers follow his basic idea
  - Software also emulates a Turing machines
    - And that makes software *very flexible*

Internet History

- When the Internet was becoming popular, only servers could be attacked
- Client software was text-based and not exploited -- until Netscape Navigator
- Today's browsers and email tools are very complex
  - And susceptible to being exploited

No One Is Safe

- In 2011, the number of large corporations successfully attacked was stunning:
  - Sony, Google, RSA, Lockheed-Martin, ...
  - Attacks are ongoing, just not as public
- These are targeted attacks and start with Windows email

Targeted Attacks

- In a targeted attack, the attacker is after some specific goal
- The attacker proceeds by:
  - Researching the target company's employees
  - Using spearphishing to email an attack
  - Using installed Trojan to reconnoiter
  - Collecting passwords for target system
  - Stealing the desired files by uploading them

Email Can Be Dangerous

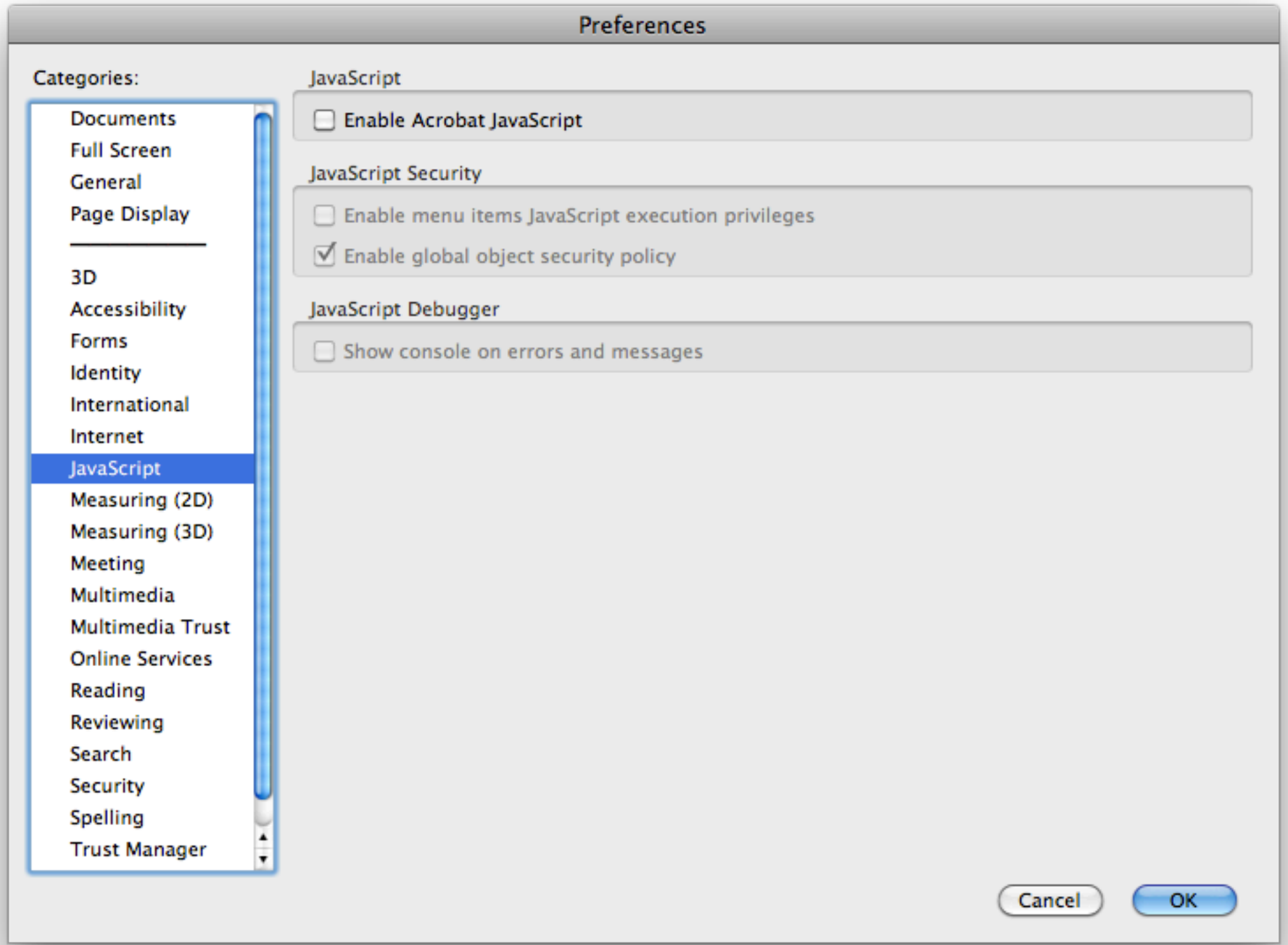
- Text-only email was safe
- Modern email readers have the display capabilities of web browsers
  - Can display images
  - Can open programs like Adobe Reader and Microsoft Word

Adobe Flash and Reader

Keep Email Reading Safe(r)

- Use an email tool that does *not* display images unless you tell it to
  - Thunderbird does this by default
- Use a spam filter, as these often will block viruses and exploits
- Disable scripting in Adobe Reader
- Don’t open attachments without thinking

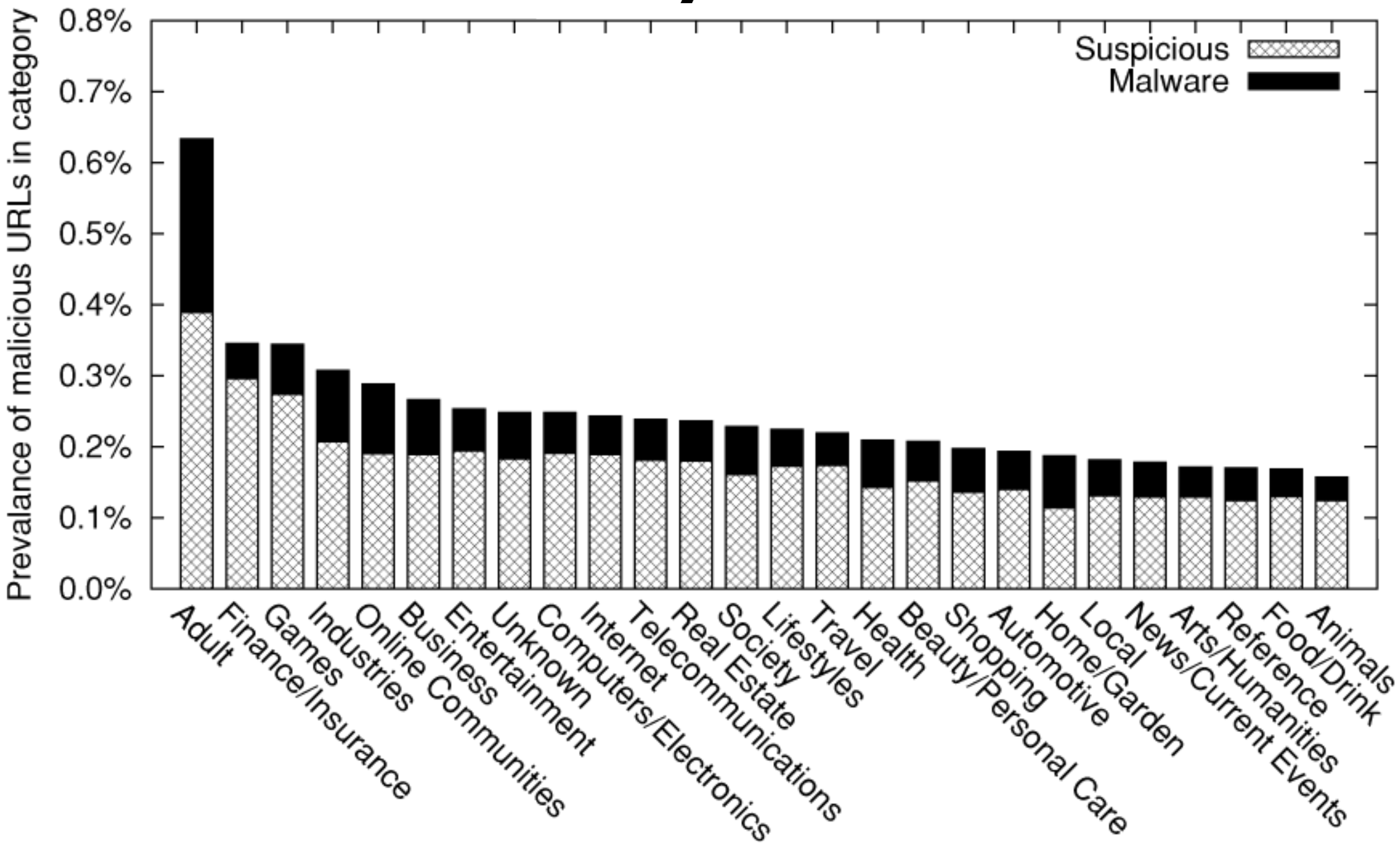
Disable JavaScript in Adobe Reader



Attacks from the Web

- Attackers also use Web servers to install malware
  - Attackers constantly search for vulnerable web servers
  - When found, they add links to their exploit sites:
    - Usually, JavaScript; sometimes Flash

Malicious Sites Can Be Anywhere



Browse Safe(r)

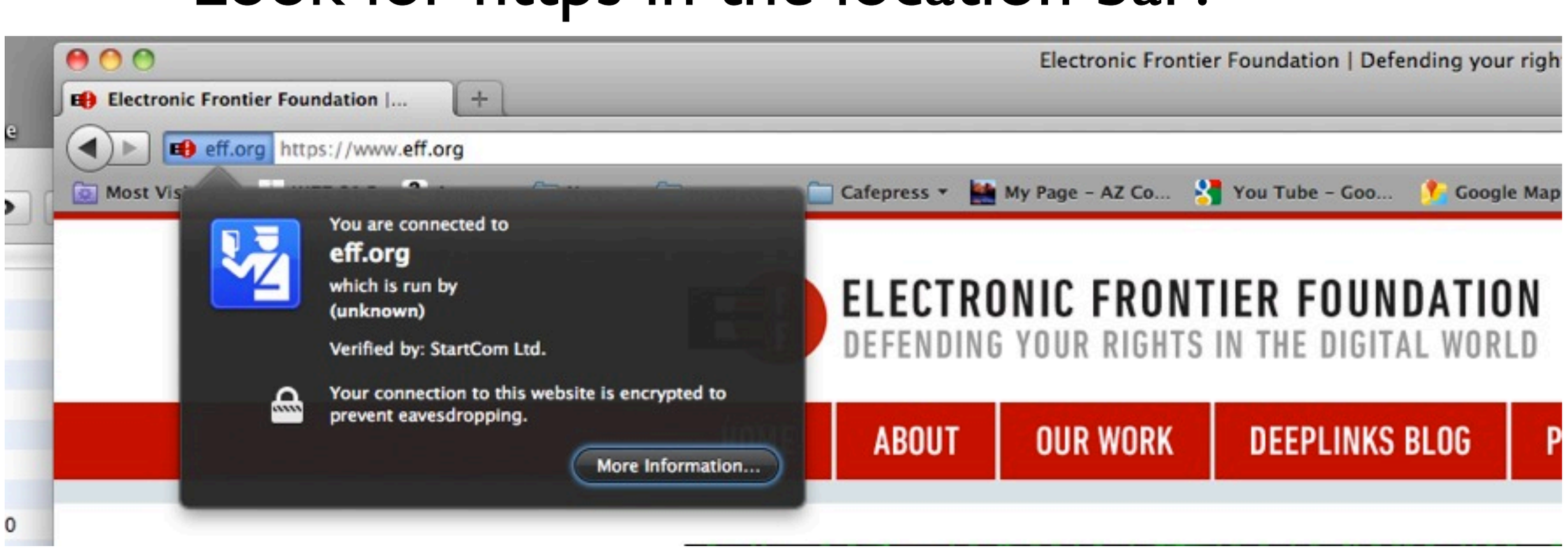
- In all browsers that you use:
  - Disable popups and third party cookies
  - Use add-ons like Adblock and Flashblock
  - Use Firefox or Chrome
    - Google actively scans for infected sites
  - Use search instead of entering URLs

More Paranoid Browsing

- Ghostery detects web bugs, allows you to block scripts, and is easy to use
- Use NoScript
  - NoScript disables all JavaScript and Flash
  - You can whitelist sites that you trust
  - You can also temporarily whitelist sites
- For email, disable HTML and JavaScript

Use HTTPS

- Use HTTPS whenever possible
- Visit eff.org, and get their https-everywhere plugin
- Look for https in the location bar:



Anti-Malware and Anti-Virus

- Anti-virus software is 20% effective
  - Two ‘new’ viruses generated every minute
  - Encryption and packing used to confuse AV
  - Malware creators use services that pack/encrypt then check malware with AV
- You still ***must*** use AV in Windows!

Fake Anti-Virus Software

- Fake AV software is still popular today
  - Malware gets installed
  - Malware displays a dialog warning of infection
  - Runs a fake scan
  - Installs more malware instead of removing any

Use Real AV

- There are many real AV companies:
  - McAfee, Symantec, F-Secure, Kaspersky, Panda, ***Sophos***, Trend Micro, BitDefender, ClamAV, perhaps 33 others
    - These companies charge money for keeping malware signatures updated daily
- Few people use Mac AV today

Microsoft Security Essentials

- As MS Windows is the most common victim of malware, perhaps they should do something?

- MS Security Essentials works for “free”:
  - Works in the background
  - Looks for malware
  - Removes known malware

Other Things You can Do

- Use accounts without Administrator privileges
  - Administrator privilege is required to make changes to the system
  - Do not enter your Administrator password while working with the Web or email
  - Switch to an Administrator account only when needed

Do Not Use Windows XP

- Windows XP is both old and dangerous
  - Almost all exploits work on XP
    - IE 6 is terribly vulnerable
- Use Windows 7 and IE 9 (or more recent) for the best security you can get with Windows

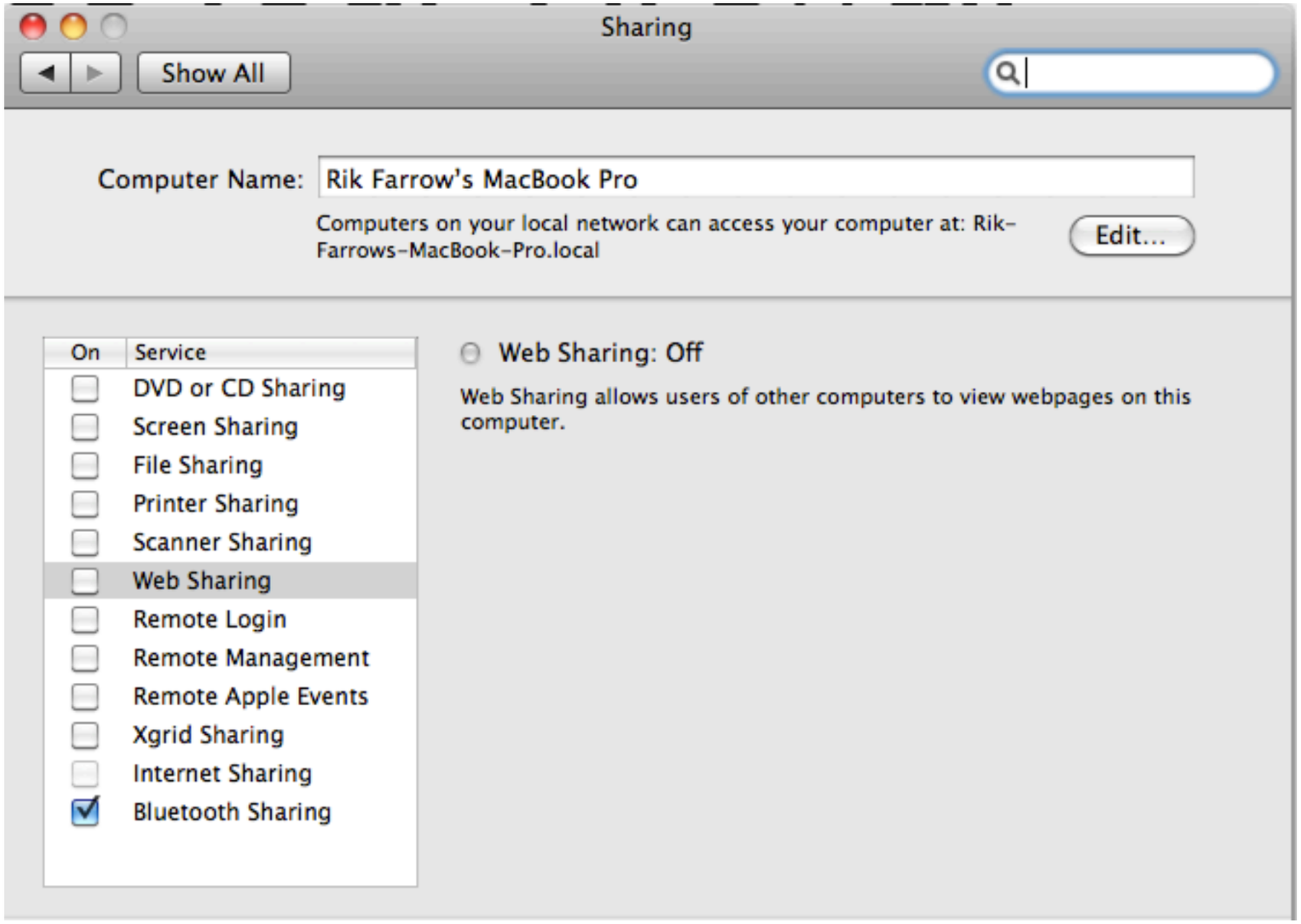
Be Cautious about What You Install

- Malware is often installed by unsuspecting users
  - Offers of free anti-virus (AV)
  - Free codecs for viewing movies
  - Plugins for Web browsers
    - Only install plugins approved by your browser vendor

Use Your Firewall

- Mac OS X includes a built-in firewall
  - It's not very intrusive
  - System Preferences->Personal->Security Firewall Tab
- Only protects against unknown services running on your Mac (like backdoors)
  - But not outward-connecting backdoors
    - Use Little Snitch for blocking these

Disable Sharing



Use a Firewall

- Most WiFI routers include a simple firewall
  - One that allows outgoing connections
    - And blocks incoming ones
    - Prevents some backdoors from working
- If you run a small business, get a real firewall and configure it conservatively