Living Safely in the New Digital World

Bob Kapell

This presentation will deal with four specific areas:

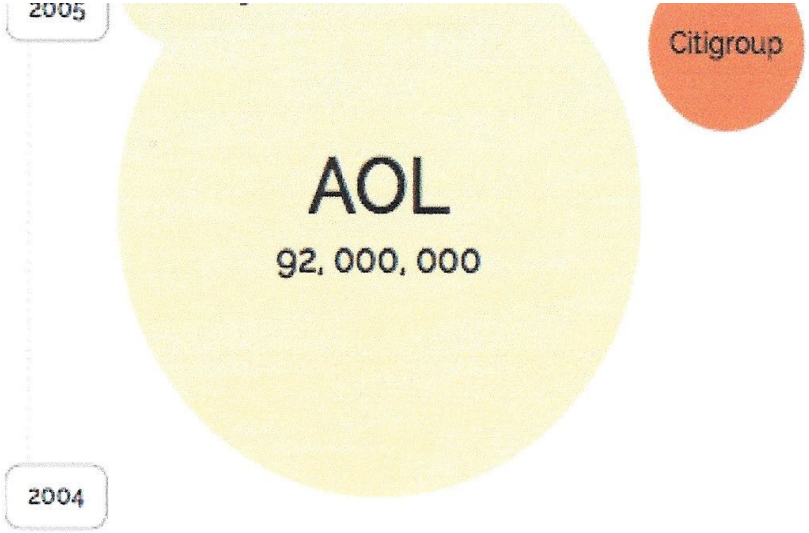
- Part 1 - The Digital “Wild West”

- Part 2 - A quick review of basic computer safety practices. (A reminder of last year’s presentation)
-
- Part 3 - Protecting your financial identity and security.
-
- Part 4 - Being careful with electronic equipment.
-
- Part 5 - Useful resources.

Part 1 - **The Digital "Wild West"**

-
- The tremendous explosion of the sale and use of Apple digital products (iPhones and iPads). In the last quarter of 2014 Apple sold 38,000 iPhones every hour!
-
- The gradual merging of the two Apple operating systems OSX and iOS. (Malware attacks on Apple computers and mobile devices)
-
- The increasing sophistication of digital malware (worms, viruses, Trojan Horses, etc. that are now being specifically written for Apple products.
-
- Last year 700,000 Apple computers were hacked through a web site that Apple App developers use to get the software to write Apps for Apple iPads and iPhones (spear phishing). These computers were infected with the "Flashback Trojan" virus which then caused all of the software that was written on these machines to be infected. The infected devices were also infected with the "WireLurker" virus.
-
- There is an ever-increasing presence of hackers and criminals on the Internet. The world's largest "market place" is the "Dark Net" (TOR)
-
- The increasing vulnerability of the Internet to hacking by computer savvy individuals, criminals and governments. In the last ten years over **one and a half billion** identities have been hacked from businesses, corporations and governments. It is estimated that at least half of these breaches include social security numbers.
-
- Very sophisticated software programs are being used to accumulate as much data as possible about everyone. These "compiler programs" search the internet for any information about an individual. The information is compiled and then the files are sold on the internet.

Data Breaches 2004-5



ORDER X-AXIS BY ALPHABETICAL DATA SENSITIVITY

SEND FEEDBACK

SEE THE DATA

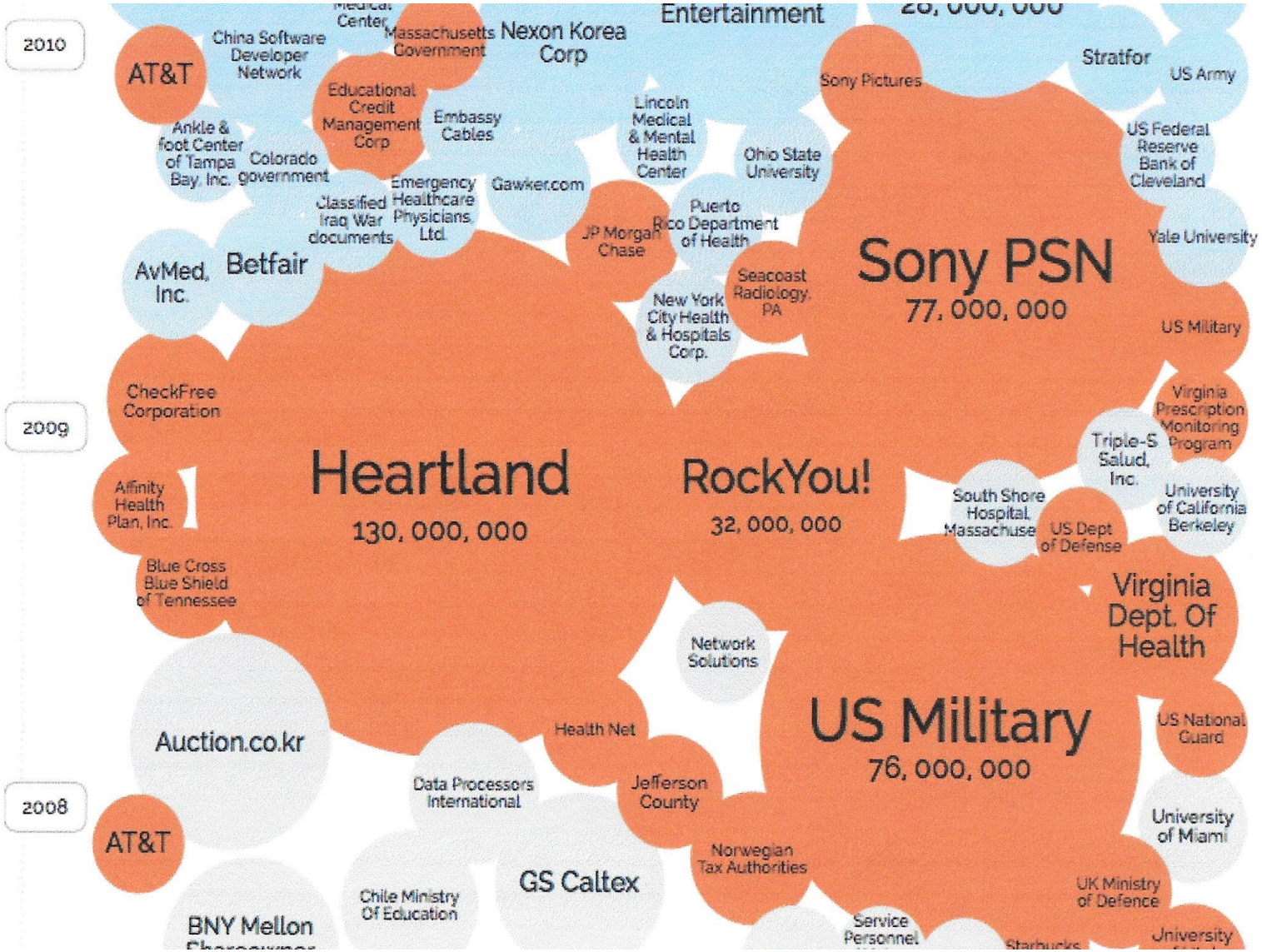
Version 1.08 // Sep 2014
previous update: May 2014
design & concept: David McCandless
code: Tom Evans,
Powered by VIZSweet

Source: DataBreaches.net, IdTheftCentre, press reports
Research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson

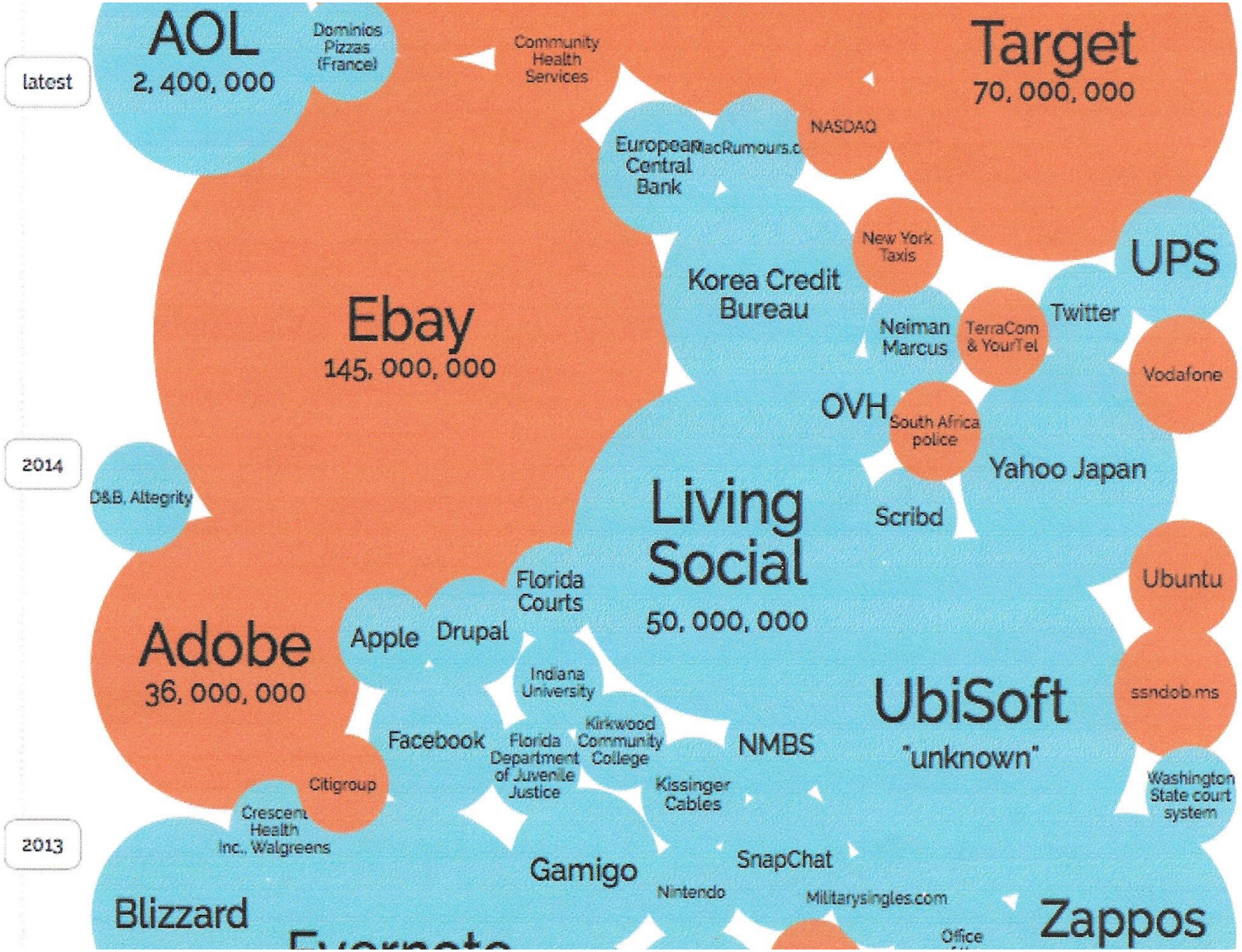
informationisbeautiful.net

VIZsweet

Data Breaches 2008-2010



Data Breaches 2013-14



TOR (THE ONION ROUTER)

XKeyscore · List of Tor hidden services · Onion routing · Free software

Onion Routing
https://www.**onion-router**.net/
This website comprises **the onion-router**.net site formerly hosted at the Center for High Assurance Computer Systems of the U.S. Naval Research Laboratory.

Go Online without Getting Snooped: Tor (The Onion Router)
www.instructables.com/.../Go-Online-without-Getting-Snoo... Instructables
In this Instructable, I'll tell you about something called **Tor** (**The Onion Router**.) I'll tell you how it works, and then offer some simple instructions on how to get your ...

Tor - The Onion Router - Reddit
www.reddit.com/r/tor reddit
TOR. subscribeunsubscribe16,810 readers. ~14 users here now ... World City Map of **Tor** Nodes. (tormap.void.gr). submitted 8 hours ago by catholic_fetishistic.

What Is Tor and Should I Use It? - Lifehacker
lifehacker.com/what-is-tor-and-should-i-use-it-1527891029 Lifehacker
Feb 21, 2014 - Dear Lifehacker, I've been hearing a lot about **Tor** these days (with a shoutout on House of Cards!), but I'm not entirely sure what it does or why ...

A beginner's guide to Tor - Digital Trends
www.digitaltrends.com › Computing
Aug 15, 2014 - You can never be too anonymous, right? If you need a basic intro into an underground way to the Web, we've got the beginner's guide to **Tor**.

Taking Stock Of Tor: Top 5 Tips For Using The Onion Router ...
www.forbes.com/.../taking-stock-of-tor-top-5-tips-for-using-the-o... Forbes
Oct 18, 2013 - The Silk Road and NSA spying may be old news, but **The Onion Router** (Tor) continues to generate interest among Internet users seeking ...

Man Behind Silk Road Website Is Convicted on All Counts

By BENJAMIN WEISER FEB. 4, 2015

A California man behind the website Silk Road, once a thriving online black market for the sale of heroin, cocaine, LSD and other drugs and illicit goods, was convicted on Wednesday of all seven counts related to the enterprise.

The verdict against the defendant, Ross W. Ulbricht, was delivered swiftly: Jurors began deliberating in the morning, and reported that they had reached a consensus about 3 1/2 hours later.

Prosecutors had portrayed Mr. Ulbricht, 30, as a "digital kingpin" who ran the website on a hidden part of the Internet, where deals could be made anonymously and without the scrutiny of law enforcement.

Evidence showed that Silk Road generated revenues of more than $213 million from January 2011 to October 2013, when Mr. Ulbricht was arrested by the Federal Bureau of Investigation in a library in San Francisco while he was logged on to his laptop as Dread Pirate Roberts, the pseudonym under which prosecutors said he operated the website. Deals were conducted in Bitcoins, and Mr. Ulbricht took millions of dollars in commissions, the government said.

Part 2 - Basic Computer Safety for Apple Users

- Use only software downloaded from the Apple Store or trusted companies. Make sure that you download the software from the company's web site. Type in the web site yourself. (Adobe Flash)
-
- Never download software or programs from an email or web site that you haven't typed in yourself. Never install software or programs or ".exe" programs from the web or thumb drives or DVDs.
-
- Set up your computer for automatic software and operating system updates. An "unpatched" machine is more likely to have software vulnerabilities that can be exploited.
-
- Choose strong passwords with letters, numbers, and special characters (if permitted). Create a different password for each important account, and change passwords regularly.
-
- Set up one "administrative" account and several "user" accounts.
-
- NEVER use the administrative account for anything except down-
- loading software programs and setting up your basic security settings.
-
- Do all of your email and web searching on a "user" account. This will help isolate any malware that you might accidently get infected with from being able to "get to" the programs themselves. (Sandboxing)
-
- Reduce the risk of the loss of important personal and financial information. Do NOT keep important financial information on your hard drive. (DON'T use your name as your Log On)
-
- Back up your machine regularly to protect yourself from the unexpected. Make sure the files can be retrieved if needed.
-
- Don't leave your computer in an unsecured area, or unattended and logged on, especially in public places. The physical security of your machine is just as important as its technical security.

- Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem "phishy." If you get a strange email request from a friend check first.
- Remember, financial institutions **NEVER** email people and request that they respond by email with their account numbers or passwords.
- Avoid untrustworthy (often “free”) downloads from freeware or shareware sites. The popular social network websites are notorious for spreading malware.
- Check email headers and web site identifiers very carefully. Any misspelling or change will indicate a **forgery**. Always type in the email address or website header yourself.
- Always use secure connections (WPA2). When connected to the Internet, your data can be vulnerable while in transit.
- Be very cautious when using wifi in a public place (coffee shop or airport). **NEVER conduct financial transactions using a public wifi.**
- Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer.
- Use the encryption tools built into your operating system to protect sensitive files you need to retain. Be careful when encrypting files.
- Use the firewall that is a part of your operating system. The firewall will help protect your computer files from being scanned.
- Install protective software when necessary**.**
  When installed, the software should be set to scan your files and update your virus definitions on a regular basis.
- Delete the cookies on Safari after every use.
- Cover your web cam when it is not being used.

Part 3 - Protecting Your Financial Security

- **New Developments in the Digital World Outside of your computer that have destroyed "privacy".**
- 1.The development and use of "advanced" malware programs. (Geeks, Criminals, Companies, and Governments)

  2. Cyber "Compiler" Programs
- **Sources of information about your identity:**
- Public records: birth records, phone numbers, voting registration, real estate records, court records, etc.
- "Self-Produced" information – entries on Facebook, Twitter, MySpace, Linkedin, online dating sites, flickr, etc. (British Intelligence Service)
- Electronic data collection programs commercial/criminal/government
- Security breaches at banks, commercial organizations, Fortune 500 companies, social networking sites, governments, etc. Over 1,500,000,000 identities have already stolen. It has been estimated by that 47% of those thefts include social security numbers.
- Uniform use of personal identities is now required for all patients under the new Affordable Health Care Act.
- **Even if you use an Apple computer, iPad or iPhone and are very careful, you can assume that your identity is already out there on the Internet. In the words of the senior executive officer of Google (Eric Schmidt): "We know where you are. We know where you have been. We probably know what you are thinking….There is no privacy anymore."**

New Threats on the Internet

-
- Open SSL
-
- “Man-in-the-Middle” attacks
-
- Stolen Authentication Keys
-
- “Wire Lurker”
-
- Credit Card “Readers”
-
- Cloud Computing
-
- Stuxnet (the first “cyber weapon”)
-
- Phishing and spear phishing
-
- Carding

- Zero Day Vulnerabilities

Hack Attack: Health insurer's customer information stolen

February 5, 2015 by Colleen Tressler Consumer Education Specialist, FTC

Last week, hackers hit Anthem, the nation's second-largest health insurance company. As many as 80 million customers had their account information stolen. The pilfered data includes names, birth dates, medical IDs, Social Security numbers, street addresses, email addresses and employment information.

If you're worried about your personal information ending up in the wrong hands, the FTC has a helpful reminder. A credit freeze, also known as a security freeze, lets you limit access to your credit report, which makes it more difficult for identity thieves to open new accounts in your name.

Our **Credit Freeze FAQs** can help you decide whether a credit freeze is right for you. One thing to remember: A credit freeze doesn't prevent a thief from making charges to your existing accounts. Even if you elect a credit freeze you still need to **monitor your existing credit card and bank accounts** for charges you don't recognize. If you decide you don't want to get a credit freeze, you can still place a **fraud alert**. It lasts 90 days — you can renew it — and makes it tougher for thieves to open new accounts.

It's also a good idea to review your credit report periodically. Federal law allows you to get a free copy every 12 months from each of the three nationwide credit bureaus. Visit **annualcreditreport.com** or call 1-877-322-8228**.** Accounts on your credit report that you don't recognize could indicate **identity theft**.

Anthem has established a **website** where members can access information about its data breach. In addition, the FTC can help you learn more about securing your **privacy and identity**.

Monitoring and Protecting Your Financial Identity

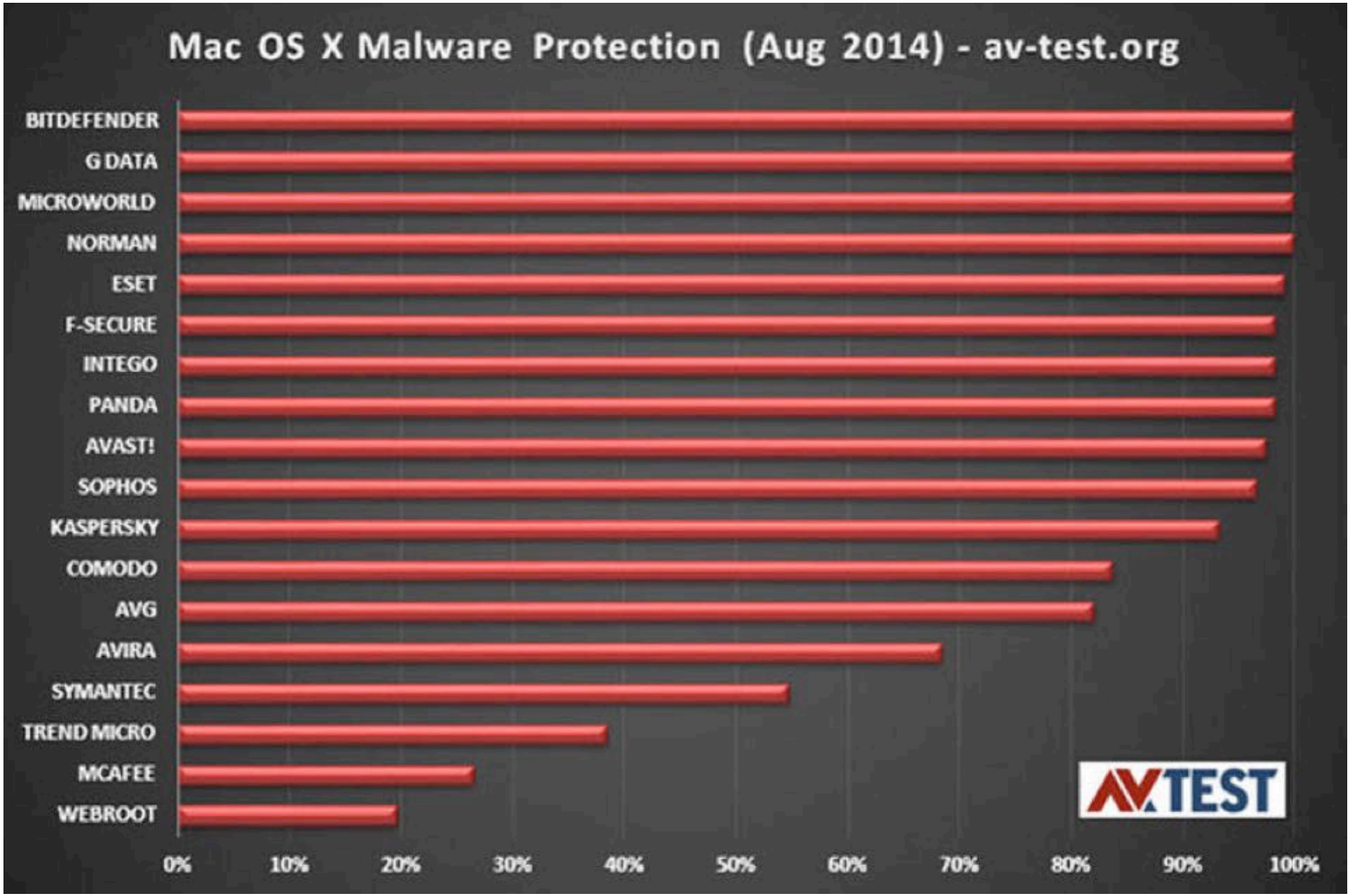
- The three credit reporting services: Experian: www.experian.com, Transunion: www.transunion.com and Equifax: www.equifax.com
- Your Annual Credit Report: www.annualcreditreport.com
- Actions: Temporary Credit Alert, Credit Freeze, "Two-Step" Program (see addendum)
- Consider the following options:
  - Using a separate user account for your financial transactions.
  - Using a separate computer for your financial transactions.
  - Use a two-step program for your financial transactions.
  - Don't use a computer for your financial transactions.

Part 4 - Being Careful With Electronic Equipment

- 1. Buying computers, tablets and smart phones.
- 2. Using electronic equipment outside the home: wireless connectivity.
- 3. Selling or discarding old electronic equipment.
- 4. Electronic equipment for the home (including home monitoring).
- 5. Electronic theft detection systems for cars.

- **Some anti-malware software for Apple machines (we are not specifically recommending these programs)**
- Sophos
- AVG
- Avast
- ClamXav
- Intego

Tests compare Mac OS X anti-malware products



“Smart” Devises for the Home

- We may want to ask some questions about devices, products or gadgets before we buy:
- Does it connect to the internet or other devices?
- What kind of information will it collect or transmit about me?
- Who will get that information?
- How will my personal information be used, stored and protected?

Part 5 - Useful Resources

- **Web Sites**
- Federal Trade Commission: www.consumer.ftc.gov
- OnGuardOnline blog: www.onguardonline.gov
- Federal Deposit Insurance Corporation: www.fdic.gov
- Internal Revenue Service: www.irs.gov
- National Consumer Protection Technical Resource Center: www.ncpw.gov
- www.apple support.com
- discussions.apple.com
- bit.blogs.nytimes.com
- www.macworld.co.uk

OnGuardOnline.gov Your Computer

The internet gives you access to countless products and services. At the same time, it can leave you open to scammers, hackers, and identity thieves. Learn experts' top tips for how to protect your information and your computer while online.

Malware
There are steps you can take to avoid, detect, and get rid of viruses and spyware.

/node-inner
/node

Disposing of Your Mobile Device
Dispose of your mobile phone safely.

Computer Security
Secure your computer and protect yourself from hackers, scammers, and identity thieves.

Securing Your Wireless Network
Steps to take to protect the wireless network in your home

P2P File-Sharing Risks
Computer security risks to consider before sharing files through a P2P network

Laptop Security
Steps you can take to prevent a thief from snatching your laptop – and all the valuable information stored on it

Disposing of Old Computers
Getting rid of a computer? Take these steps to protect your personal information.

Laptop Security Bookmark
Steps you can take to keep your laptop from getting lost or stolen

Relevant Articles

- A Two-Step Plan to Stop Hackers by Ron Lieber
-
- Are We Puppets in a Wired World by Sue Halpern

  Best Mac antivirus software 2014 by Andrew Harrison (www.macworld.com.uk)
-
- Flaw Found in Key Method for Protecting Data on the Internet by Nicole Perlroth
-
- Is That Gadget Internet Connected by Cristina Miranda
-
- Keeping Swindlers Out of Your Bank and Brokerage Accounts by Paul Sullivan
-
- Report Analyzes Extent of Data Breaches in California by Nicole Perlroth
-
- Selling Secrets of Phone Users to Advertisers by Claire Cain Miller and Somini Sengupta
-
- Sidestepping the Risk of a Privacy Breach by Ron Lieber
-
- Tests compare Mac OS X anti-malware products by Larry Seltzer (www.zdnet.com)

Computer Books

- Big Data: A Revolution That Will Transform How We Live, Work and Think by Viktor Mayer-Schönberger & Kenneth Cukier
- * Cyber Security and Cyber Warfare by Peter Singer and Allen Friedman
- * Dark Market: Cyber Thieves, Cyber Cops and You by Misha Glenny
- * Hacking the Future: Privacy, Identity and Anonymity on the Web
- by Cole Stryker
- The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution by Walter Isaacson
- I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy by Lori Andrews
- * The Internet Police: How Crime Went Online — and the Cops Followed
- By Nate Anderson
- The Net Delusion by Evgeny Morozov
- * The New Digital Age: Transforming Nations, Business and Our Lives by Eric Schmidt & Jared Cohen
- Predicitive Analytics The Power to Predict Who Will Click, Buy or Die
- by Eric Siegel
- * Privacy and Big Data: The Players, Regulators and Stakeholders
- by Terence Craig and Mary E. Ludloff
- Social Networks and the Death of Privacy by Lori Andrews
- Zero Day: The Threat in Cyberspace by Robert O"Hara