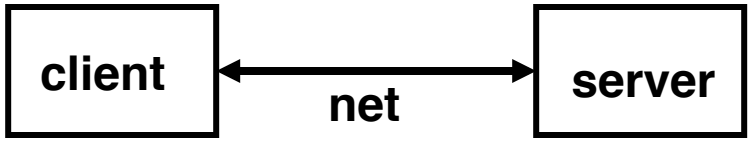
Privacy, security, self-defense

- what can go wrong
- what you can do about it for yourself
- what we should do about it as a society / country / ...

Potential security & privacy problems



- **attacks against client**
  - release of client information
    cookies: client remembers info for subsequent visits to same server
  - adware, phishing, spyware, ransomware, viruses, ...
    spyware: client sends info to server upon connection
    often from unwise downloading
  - buggy/misconfigured browsers, etc., permit vandalism, theft, hijacking, ...
- **attacks against server**
  - client asks server to run a programs when using cgi-bin
    server-side programming has to be careful
  - buggy code on server permits break-in, theft, vandalism, hijacking, …
  - denial of service attacks
- **attacks against information in transit**
  - eavesdropping
    encryption helps
  - masquerading
    needs authentication in both directions

Privacy on the Web

- **what does a browser send with a web request?**
  - IP address, browser type, operating system type
  - referrer (URL of the page you were on)
  - cookies
- **what do "they" know about you?**
  - whatever you tell them, implicitly or explicitly (e.g., Facebook)
  - public records are really public
  - lots of big databases like phone books
  - log files everywhere
  - aggregators collect a lot of information for advertising
  - spyware, key loggers and similar tools collect for nefarious purposes
  - government spying is everywhere
- **who owns your information?**
  - in the USA, they do; you don't
  - much less so in the EU (GDPR, May 2018)

General Data Protection Regulation (GDPR) (May 2018)

You have the right to:

- **information** about the processing of your personal data;
- **obtain access to** the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be **corrected**;
- request that personal **data be erased** when it's no longer needed or if processing it is unlawful;
- **object** to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the **restriction** of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller ('**data portability**');
- request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights_en

Worms and viruses

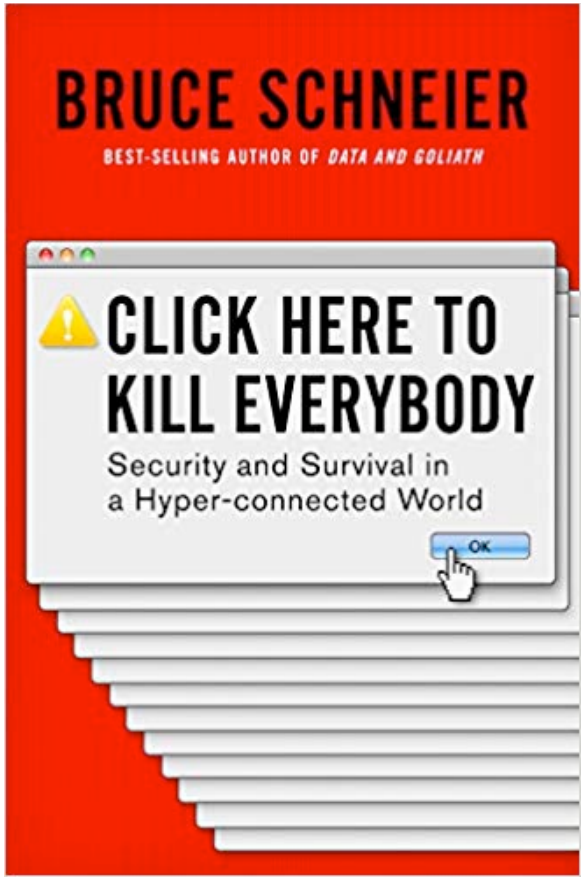
- **old threat, new technologies**
  - new connectivity makes them more dangerous
- **basic problem: running someone else's software on your machine**
  - bugs and ill-advised features make it easier
- **operates by hiding executable code inside something benign**
  - e.g., .EXE file or script in mail or document, downloaded content
  - USB drive or other attractive medium
- **Melissa, ILoveYou, Anna Kournikova viruses use Visual Basic**
  - applications (Word, Excel, Powerpoint, Outlook) have VB interpreter
  - a document like a .doc file or email message can contain a VB program
  - opening the document causes the VB program to be run

- **virus detectors**
  - scan for suspicious patterns, suspicious activities, changes in files
  - this is a real arms race

Internet of Things

- you thought it was bad with computers
- phones made it worse
- and now it's the Internet of Things

- lots and lots of Things
- most have very poor security
- usually no incentive to improve
- usually no mechanism to upgrade or update

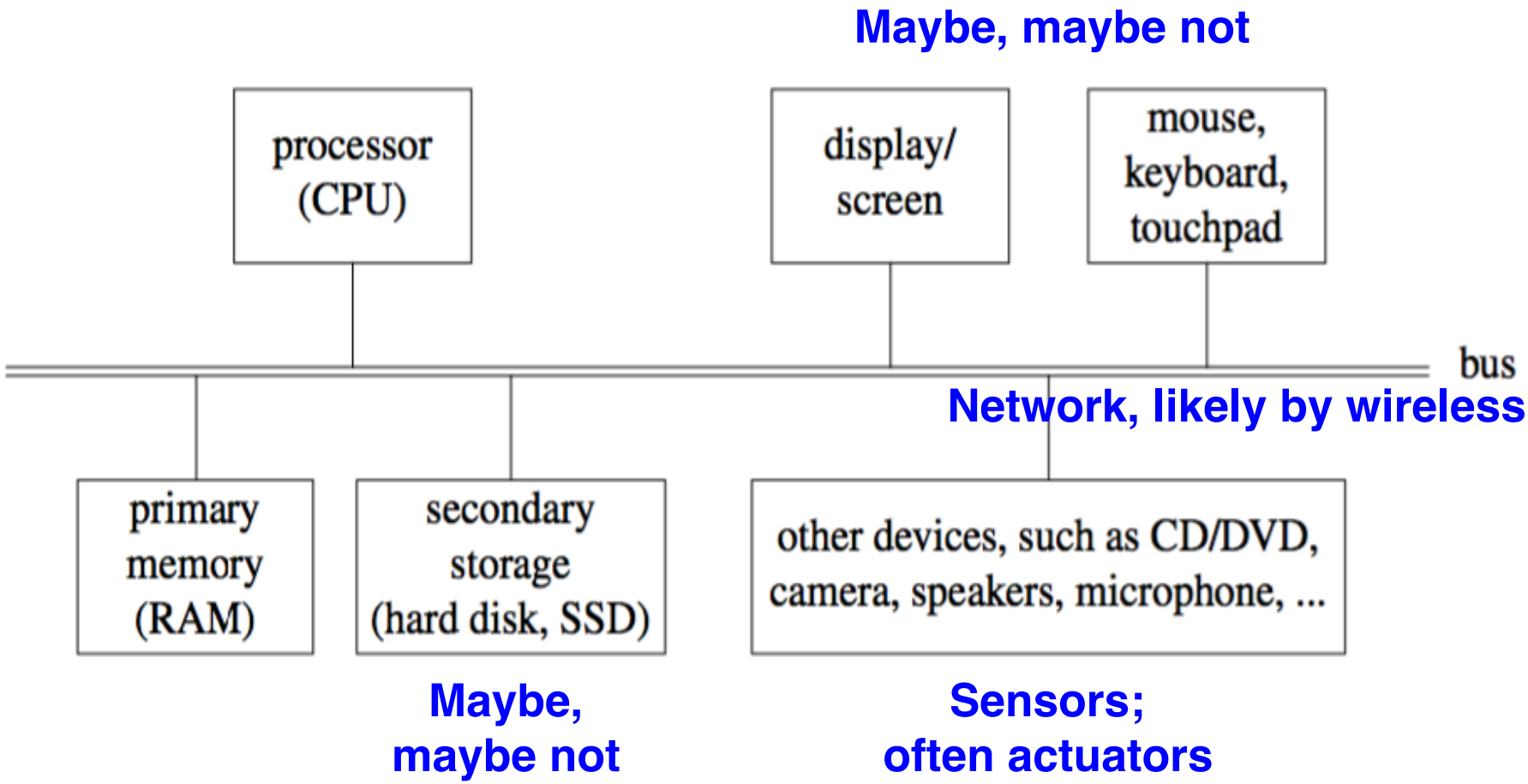


Internet of Things

- vacuum tubes => transistors => integrated circuits
- magnetic cores => integrated circuits
- mechanical disks => solid state drives
- copper wire => fiber optics
- wired Ethernet => wireless

- smaller, cheaper, faster, better => lots of things
- things + wireless + Internet => Internet of Things

Thing architecture



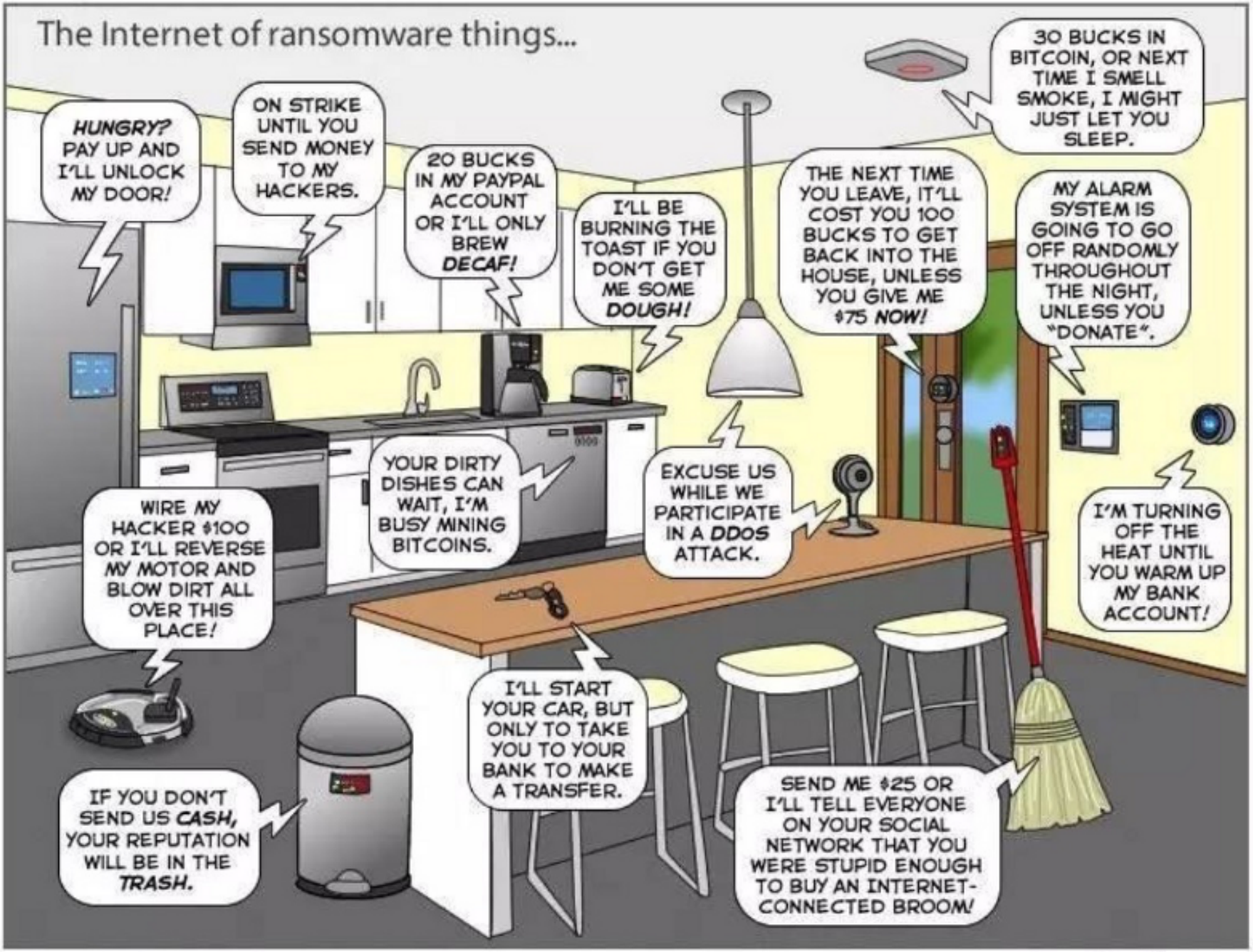
Lots of Things

Cheez-It Dash Button
Amazon
$4.99 Prime

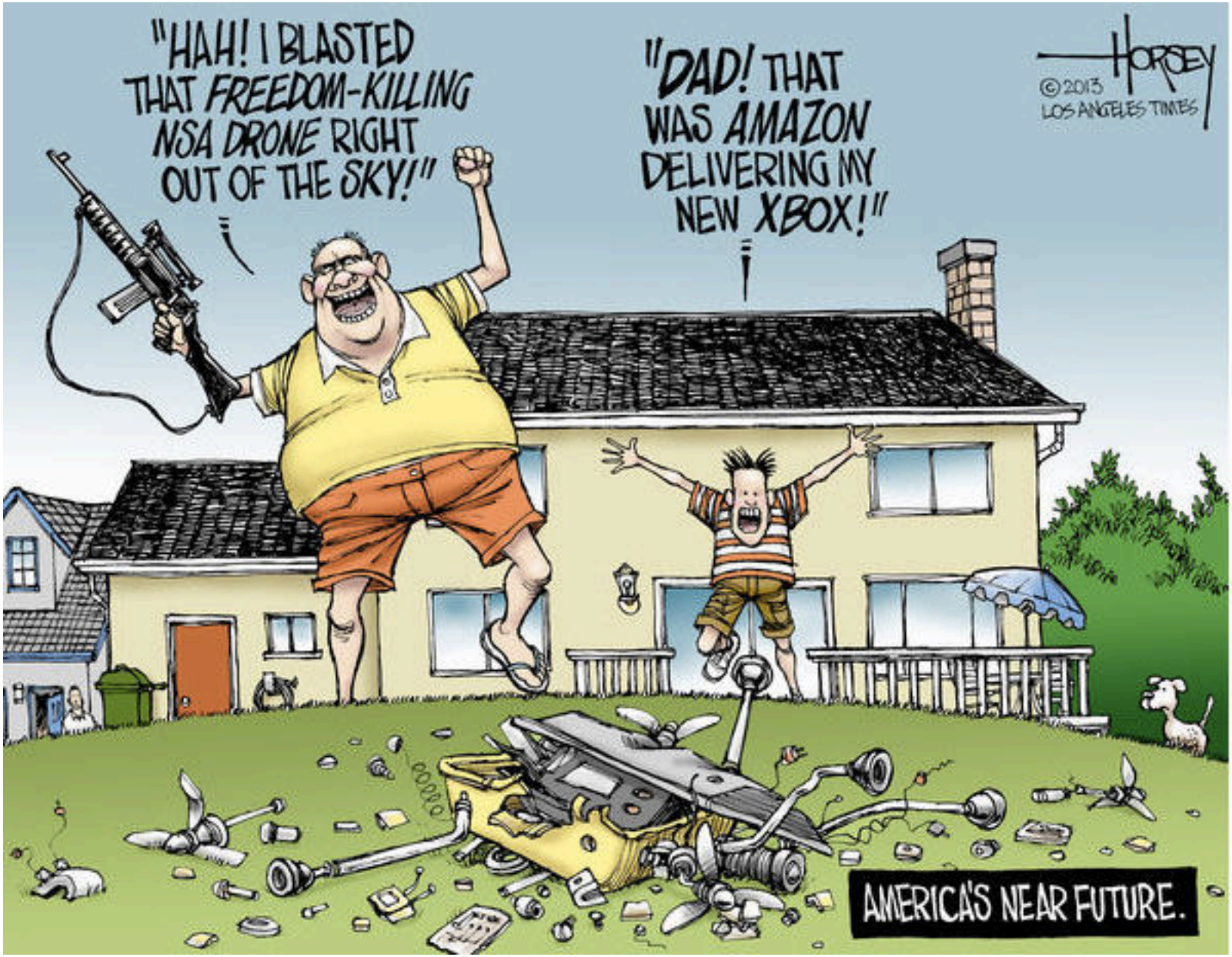
Pop-Tarts Dash Button
Amazon
$4.99 Prime

- **home**
  - web cams, baby monitors, ...
  - lights, thermostats, door locks, ...
  - TV, appliances, ...
- **personal services and gadgets**
  - games & toys, e-readers, watches, Fitbit, ...
  - Alexa, Siri, Google Voice, ...
- **cars, trains, planes, drones**
- **medical devices and instruments**
- **infrastructure**
  - power plants and grid, traffic lights, transportation,
  - phones & communications systems, ...
- **manufacturing, shipping, ...**
- **police & military systems**
- **. . .**

The Joy of Tech™ by Nitrozac & Snaggy

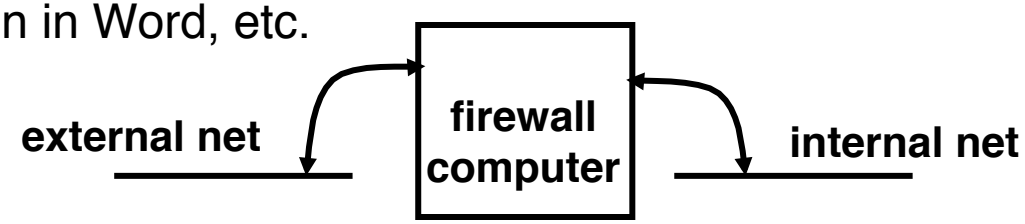


joyoftech.com


"HAH! I BLASTED THAT FREEDOM-KILLING NSA DRONE RIGHT OUT OF THE SKY!"
"DAD! THAT WAS AMAZON DELIVERING MY NEW XBOX!"
HORSEY
©2013 LOS ANGELES TIMES
AMERICA'S NEAR FUTURE.

Defenses

- **use strong passwords; don’t share them across important accounts**
- **use 2-factor identification when available (e.g., Duo)**
- **cookies off, spam filter on, Javascript limited**
- **turn off previewers and HTML mail readers**
- **anti-virus software on and up to date**
  - turn on macro virus protection in Word, etc.
- **run spyware detectors**
- **use a firewall**



- **try less-often targeted software**
- **be careful and suspicious all the time**
  - don't view attachments from strangers
  - don't view unexpected attachments from friends
  - don't just read/accept/click/install when requested
  - don't install file-sharing programs
  - be wary when downloading software