Ethics / Crime / Security

Ethics

- Some key issues
  - Ethics / Computer ethics
    - People's ethics change behind a keyboard
  - Electronic waste…
  - Digital divide
  - Information privacy / security
    - Target, chip and PIN
  - Identity theft
    - Happens every two seconds,
    - Cost of $25 billion, 2012

Ethics

- Electronic Waste
  - With the explosion of IoT devices, we run the risk of an explosion in electronic waste and harmful materials
    - We've already experienced it
  - Before we get to statistics, let's take a look at some images that illustrate the impact of electronic waste on developing countries:

Ethics

Ethics

Ethics

Ethics

- Electronic Waste
  - Ghana, Nigeria, India, China, among many others, are used as tech dumps
  - Some stats:
    - 1.6 billion cell phones manufactured in 2012
    - Average American keeps phone 18 months
    - 60% of eWaste ends up in landfills
    - 30% is non-recyclable

Source: ifixit.org

Ethics

- Recent large-scale hacks
  - IRS, May 2015, 330,000 users' data stolen
  - Office of Personnel Management, ongoing hack discovered June 2015, every federal employee and retiree affected, plus 1 million former workers
  - Anthem, March 2015, 80 million users' info stolen
  - iCloud, ~Sept. 2014, celebrity photos stolen

Ethics

- Recent large-scale hacks
  - Target
  - Ashley Madison, discovered July 2015, 37 million users' data stolen (and posted)
  - Sony, December 2014, 100 terabytes of internal data
  - Sony, May 2011, 20,000 users' personal and financial information stolen
  - Sony, April 2011, 70 million users' accounts, passwords, and bank information

Ethics

- We think about security differently online then off
- With IoT, we don't think about it at all
  - We barely consider it with regular devices
  - As was seen with the recent Dyn attack, IoT devices are now a significant new vector for malicious code and actors

Ethics

- How people maintain their security, privacy and identity online
  - Secure / monitored / verified websites
  - The privacy / security policy
  - Cookies
  - Anonymous surfing
  - Opt-out emails
- With IoT, these are not options

Ethics


VeriSign
Secured

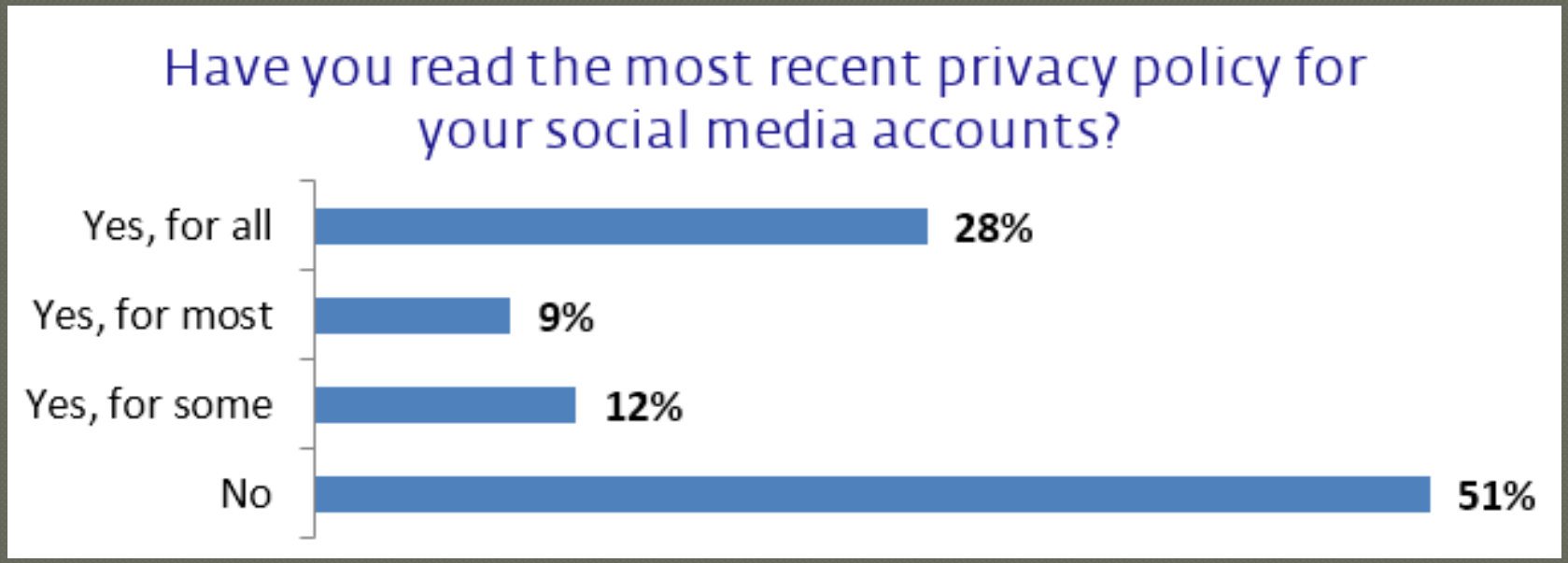

Norton
SECURED
powered by VeriSign


GeoTrust
SECURE SITE

Ethics

- How to maintain your security, privacy and identity online
  - Secure / monitored / verified websites
  - The privacy / security policy
  - Be careful about cookies
  - Anonymous surfing, if necessary
  - Opt-out emails

Ethics


Have you read the most recent privacy policy for your social media accounts?
Yes, for all
28%
Yes, for most
9%
Yes, for some
12%
No
51%

Ethics

- Information and image accuracy
  - Technology can be used to portray unrealistic images / abilities
  - Inconsistency of stored data
- Information property
  - Intellectual property / fair use
  - Data privacy
  - Spam, spyware
  - Cybersquatting

Ethics

- The need for an ethical code of conduct
  - Many organizations have distinct ethical guidelines
  - Technology companies do as well
  - Responsible use of technology
  - computer crime

Crime

- Computer Crime
  - Definition
  - The computer access debate
  - Unauthorized computer access
  - Laws
    - Computer Fraud and Abuse act of 1986
    - Electronic Communications Privacy Act of 1986
    - The Identity Theft and Assumption Deterrence Act of 1998

Crime

- Information Accessibility
  - What is it?
  - Carnivore, DCSNet
  - ECPA
  - Eligible receiver
  - Who owns, and has a right to examine, email messages, especially now?

Crime

- Computer crime (con't)
  - Computer forensics
  - Hacking / black hat / white hat
    - Risks of the Internet of Things
  - Cyberwar / Cyberterrorism
    - Pentagon reports 10 million attempts / day
    - http://map.norsecorp.com/
  - Vigilantism / digital activism (hacktivism)
  - Who does this?

Crime

- Computer crime (con't)
  - Cyberbullying
  - Digital threats and harassment
  - Shaming
  - Laws are ineffective, sometimes nonexistent
    - Especially with IoT
  - Education and awareness campaigns are most effective

Security

- Piracy
  - Has been around for a very long time
  - Costs companies billions
  - $53 Billion globally, conservatively (2011)
  - Microsoft: $22 billion for malware, $114 billion for cyberattacks (2013)
  - In 2010, 95 percent of music downloads were done illegally (International Federation of the Phonographic Industry)

Security

- Piracy
  - File sharing / Physical counterfeiting
  - Creates an ‘everything should be free mentality’
  - Facilitated by distribution costs as compared to production costs for digital goods
  - Combatted somewhat with the rise of iTunes
  - Movie downloaders wealthier, more willing to go to movies, stop behavior if it hurts the industry

Security

- Common compromise vectors
  - Unauthorized access
    - Information modification
    - Denial of service
    - Remote access
    - Zombie computers / botnets
      - Ramifications

Security

- Common compromise vectors
  - Unauthorized access
    - Information modification
    - DDoS / Zombie/botnets
  - Malware – externally supplied, internally acted
    - Viruses
    - Worms
    - Trojan horses (Logic bomb)
    - Evil twins
    - Keyloggers
    - Ransomware

Security

- Common compromise vectors (cont)
  - Spyware, Spam, Spoofing
    - Adware
    - Spam
    - Phishing – especially dangerous
    - The Dark Web
    - Pharming
    - 419 scam

Security

- How is it done?
  - It's not easy
    - (sometimes it is)
  - Known / Unknown exploits
  - Physical / remote access
  - Wired / wireless
  - Zero day / established faults
  - Target / vector
  - Always requires specific tools

Security

- How is it done? (Not Easy!)
  - Specific OS's can be used
  - Shell code
    - Buffer attacks
    - Use after free
    - Heap spray
    - NOP slide / sled
  - PKI attacks (Man in the middle)
  - SQL Injection
  - PW attacks
  - Shack attacks
  - Social engineering

The Stack:

- Function call
- Passed parameters
- Return address*
- Local variables
- Registers (a,b,c,d)

Security

- What can be done?
  - With IoT devices, process can be easy
    - Name change example
  - Many have limited, or no, security built in
  - Physical unclonable functions (PUFs)
  - Do standard network security practices work?

Security

- What can be done?
  - With IoT devices, process can be easy
    - Name change example
  - Many have limited, or no, security built in
  - Physical unclonable functions (PUFs)
  - Do standard network security practices work?

Security

- Three categories of security
  - Physical
  - Logical
  - Behavioral

Security

- Access control (Authentication)
  - Passwords
  - Tokens
  - Smart cards
  - Biometrics
  - Encryption

Worst Passwords from 2015

1. 123456 (Unchanged from 2014)
2. password (unchanged)
3. 12345678 (↑ 1)
4. qwerty (↑ 1)
5. 12345 (↓ two)
6. 123456789 (unchanged)
7. football (↑ 3)
8. 1234 (↓ 1)
9. 1234567 (↑ 2)
10. baseball (↓ 2)
11. welcome (new)
12. 1234567890 (new)
13. abc123 (↑ 1)
14. 111111 (↑ 1)
15. 1qaz2wsx (new)
16. dragon (↓ 7)
17. master (↑ 2)
18. monkey (↓ 6)
19. letmein (↓ 6)
20. login (new)
21. princess (new)
22. qwertyuiop (new)
23. solo (new)
24. passw0rd (new)
25. starwars (new)

Security

- Encryption
  - Many types, for data in all states
  - Usually algorithmic
    - Public key (PGP)
  - Wireless encryption
    - WEP/WPA/WPA2
    - WIFI protected setup

Security

- Physical ailments
  - Carpal tunnel syndrome
  - Repetitive stress injury
  - Technostress