If the NSA Is Already Listening, Do I Still Need to Secure My Phone and Computer?

David Rusting, CISO
University of California Office of the President

YES

Overview

- Information Security
- Trends in Cyber-Security Threats
- Leading Risk Vectors
- What can I do?
  - As a general user
  - As a system administrator

What is Information Security?

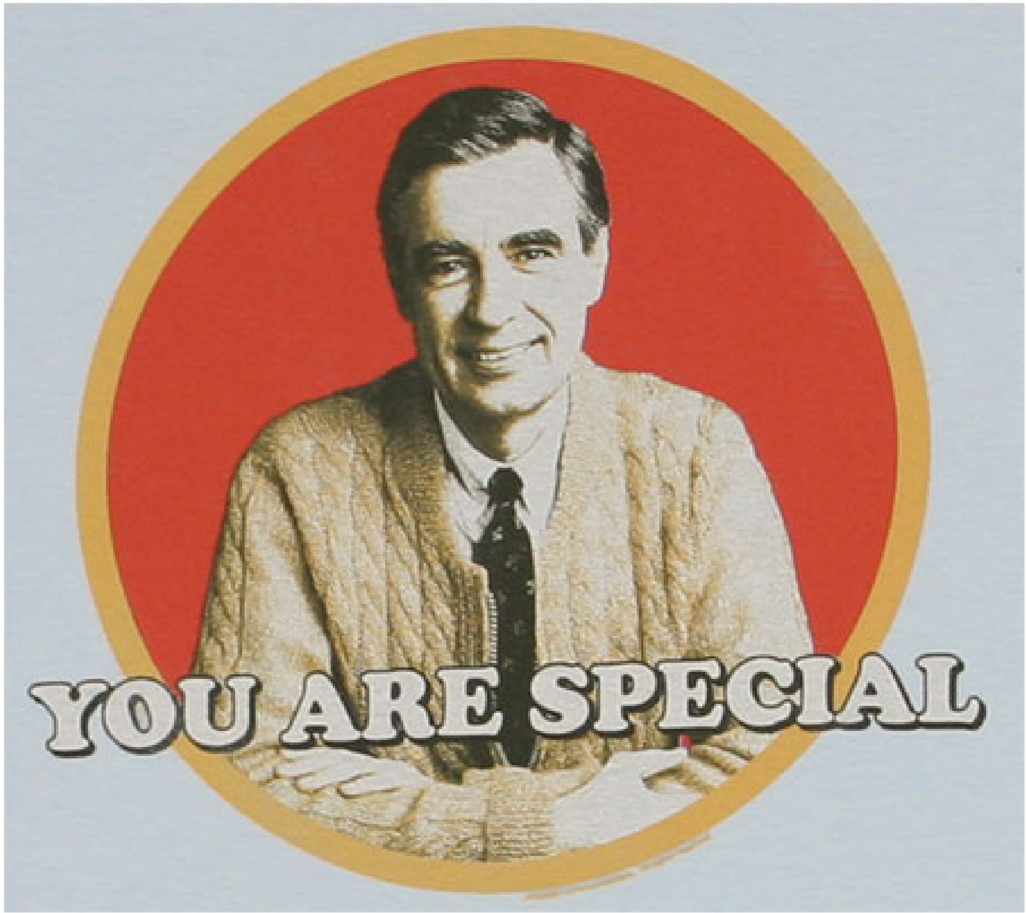
- Information security supports the protection of information resources from unauthorized access, which could compromise their confidentiality, integrity, and availability.

- Information resources: infrastructure (such as computers and networks) and information (whether or not it is related to individuals).

- Information security is essential for autonomy privacy (“right to not be observed”) and information privacy (“protection required by law or policy”).

Security
Management
Network
Design
Data
firewalls
Compliance
Scanning
eDiscovery
Intrusion
Encryption
Loss
Mobile
Threat
Assessments
Detection
Support
Risk
Application
Development
System
Analysis
Response
Research
Certificates
Prevention
Standards
Event
Protection
Endpoint
IDS
Architecture
SSL
Assessment
Awareness
Guidance
Host
Audit
Egress-point
Outreach
Enterprise
Strategy
Device
Vulnerability
forensics
Project
Policy
Malware
Incident

WHY?


YOU ARE SPECIAL

Who you are
What you do
Where you work
How you work
How you live

YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Trending Threats in Higher Education

- Significant increases in breaches*
  - 2011: 572,000 records
  - 2012: 1,730,000 records
  - 2013: 2,800,000 records

- Breaches of records in the ***past 120 days alone****
  - University of Maryland: 309,079
  - North Dakota University: 290,780
  - Indiana University: 146,000

- Coming soon…your breach in the news
  - Public visibility and scrutiny is increasing
  - Social media and “instant broadcast”

*Source: Privacy Rights Clearinghouse

UC is not immune

- UCSF– 10,000 records this past March
- UC Davis Health System – 1,800 in January
- UCLA Health System – 16,000 in 2011
- UCB – 160,000 in 2009
- UCLA – 800,000 in 2006

- UC stewards data:
  - 65,000 retirees
  - 180,000 employees
  - 5,000,000 students – past and current
  - Millions of patients

- Obligation to preserve the public trust

What’s it worth?*

- Social Security number: $1-3
- Facebook: $2.50
- Apple ID: $8
- Credit Card: $20
- Medical Record: $50
- Tax Fraud /Identify Theft: $3,400

- The number one group targeted for tax fraud / identity theft: ***students***
  - 50% higher than elderly, children and deceased – ***combined***

UNIVERSITY
OF
CALIFORNIA

*Sources: KrebsOnSecurity, RAND National Security Research Division, Medical ID Fraud Alliance, US GPO, US Dept. of Treasury

Leading Risk Vectors

- Lost and stolen devices
- Compromised credentials (“phished”)
- Compromised devices (“hacked”)
- Insider (accidental or nefarious)

What can I do as a general user?

- Encrypt devices used for UC business – no matter who bought them
- Encrypt your smartphone or tablet – no matter who bought it
  - Connecting to Exchange does this easy-peasy ☺
- Make your UC password different from other passwords
- Report anything that does not pass the “gut” test
  - Emails asking for passwords
  - People you don’t know asking for access
  - Data in places it should not be

What can I do as a system administrator?

“Seven Steps to Security”

- ***W*** hitelist connections or applications
- ***E*** nsure patching of systems and applications
- ***A*** ccess and unusual event monitoring
- ***V*** ulnerability test systems and applications
- ***E*** xposed to the world, so harden it!
- ***R*** otate system admin password quarterly
- ***S*** eparate accounts for sysadmin vs. general work – with different passwords

Thank you

and Q&A