Security: Why it’s important to you
• Adam Godwin
  – 5 Years of Experience in IT security
  – M.S. in System Engineering
  – CISSP
  – Security Analyst for UTIA
Topics

• Why it’s important to you
• UTIA security program
• Types of data (classification)
• Quick tips
• Take away
“The most misused SSN of all time”
078-05-1120

1938
E.H. Ferree

1943
5,755 people

1977
12 people
Somebody’s Watching You
We Are Under Attack
They Want Your Identity

Name: John Brown
Social Security Number: 999-99-999
Email: jbrown32@utk.edu
Email Password: br549
Instant Messenger: JohnB32
Instant Messenger Password: br549
How to Protect Yourself

• Identity Theft
• How do thieves steal an identity?
  – Dumpster Diving
  – Skimming
  – Changing Your Address
  – Old-Fashioned Stealing
How to Protect Yourself

• **First**, set up free fraud protection alerts
  – Credit Reporting Agencies:
    • **Equifax**: www.equifax.com
    • **Experian**: www.experian.com
    • **TransUnion**: www.transunion.com
• **Second**, do it again in 90 days
• **Third**, remove your name from pre-approved credit card and junk mail lists
  • www.optoutprescreen.com
• **Fourth**, order free credit reports
(1) "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

(2) “Information holder” means any person or business that conducts business in this state, or any agency of the State of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information.

(3) "Personal information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:
   (i) Social security number;
   (ii) Driver license number; or
   (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
McAfee Reports 200 New Computer Attacks Per Minute in 2013

March 11, 2014  No Comments

A new report from McAfee says every minute there are more than 200 new computer attacks using a variety of malware.

The report, *McAfee Labs Threats Report: Fourth Quarter 2013*, noted an increase in Point of Sale attacks, citing Target. McAfee says that it now "has gained an understanding of the exact malware used in this attack." McAfee says the type of "off the shelf" attack on Target Corporation was a simple text file and the class of attack was "far from advanced."

The McAfee report noted that after stealing the credit card data they sold it in batches of one to four million at a time. "One popular credit card black market is the Lampeduza Republic," the report noted. "Its well-organized hierarchy and documented constitution make for a disciplined and functional marketplace. Lampeduza’s network of sales websites is very active and contains many logs specific to these recent retail attacks. Thieves can pay for the stolen credit cards using one of the many anonymous virtual currency mechanisms, such as Bitcoin."

The report said criminals behind the campaigns are particularly dangerous and McAfee doesn’t see the issue going away anytime soon. "We believe these breaches will have long-lasting repercussions," the report said. "We expect to see changes to security approaches and compliance mandates and, of course, lawsuits. But the big lesson is that we face a healthy and growing cybercrime industry."

McAfee also noted a significant increase in malware and ransomware attacks on mobile devices. It collected 2.47 million new Android sample attacks in 2013, a 197 percent increase over 2012. Ransomware attacks, where the virus shuts down the application until the owner pays a ransom to the hacker, doubled from the fourth quarter of 2012 to 2013, according to the report.
Kansas Suspends State Tests Following Cyber Attacks

By Benjamin Herold on April 2, 2014 3:08 PM

The Kansas State Department of Education suspended the administration of state exams on Wednesday after its testing vendor was overwhelmed by attacks from unidentified hackers.

While the cyber strikes scuttled the testing schedules of hundreds of schools across the state and left state officials scrambling to upgrade their security infrastructure, the full fallout is not yet known.

“We’re still in 'fix-it mode' right now,” said Marianne Perie, the director of the Center for Educational Testing and Evaluation, or CETE, which develops and administers the exams. “We’re putting out the fire before we have a chance to assess the damage.”
Security & Risk Management

Paranoia

Prevention

Directive

Voluntary

Response

Complacency

Balance

Risk Management
Security & Risk Management

- Security
- Efficiency

Risk Management
UTIA security

• Based on NIST & FIPPS 199 standards
  – Confidentiality, Integrity, Availability
• Security website
  – https://utia.tennessee.edu/Security/SitePages/Home.aspx
Data Classification

- Data classification based on NIST & FIPPS 199 standards
- Three types
  - Low
  - Moderate
  - High
Data Classification

• Low Data
  – Anything not classified as moderate or high
Data Classification

• Moderate Data
  – Examples include SSN, proprietary, medical information such as lab results, credit card information, protected research data, other legally protected data.
Quick Tips

- Identity Finder
Quick Tips

• Emails
  – Links
    • To click or not to click
  – Spam emails
    • Is there any other kind
  – Attachments
    • Good or bad
  – Secure email
    • OIT Vault
Quick Tips

• Updates
  – Windows Updates
  – MAC updates
  – Adobe
  – Java
Quick Tips

• Antivirus
  – Malwarebytes
    • Updates
    • Scanning
  – Microsoft System Center Endpoint Protection (MSCEP)
    • Updates
    • Scanning
Quick Tips

• SNAP scans
  – https://remedy.utk.edu/snap/
  – Online tool for security scan
    • Show points of entry and possible compromises
  – Only Knoxville and UTIA machines can use it
    • Must log in with your NETID and password
Take Away

• Know what type of data you have on your machine
• Keep everything updated
• Review emails carefully
• Schedule weekly scans (Malwarebytes and/or MSCEP)
Take Away

• Malwarebytes download
  • https://ag.tennessee.edu/Pages/malwarebytes.aspx

• SNAP scans
  • https://remedy.utk.edu/snap/

• OIT software download site
  • https://web.dii.utk.edu/softwaredistribution/
    – Microsoft System Center Endpoint Protection (MSCEP)
    – Identity Finder
Questions & Discussions