INTERNET SAFETY FOR SURVIVORS OF BRAIN INJURY

CHRISTOPHER JARKO
GSEC, GMON
COMMUNICATIONS SYSTEMS AND NETWORKS ANALYST

OVERVIEW

- **Introduction – Who I Am and Why I Care**
- **Internet Safety Versus Internet Security**
- **The Risk: Do We Really Have any Information Worth Stealing?**
- **The Threat: Social Engineering: How and Why it Succeeds**
- **The Vulnerability: Special Considerations for Brain Injury Survivors**
- **How We Can Help**
- **10 Tips**
- **Question & Answer Period**

INTRODUCTION

- **About Me:**
  - **27+ years with the Department of Defense**
    - **20 Years active duty USAF (Nuclear Operations, Treaty Verification, Plans & Policy, and Command & Control)**
    - **1 year as a contractor (Strategic Planner)**
    - **6 ½ years as a Civil Servant (Cybersecurity Planning & Analysis)**
    - **...But I am <u>not</u> speaking in that capacity today!**
  - **Candidate for MS in Information Security Management from SANS Technology Institute**
  - **I do not have a technical background, but I am proficient in technical aspects of cybersecurity**
- **Why I Care:**
  - **Brain injury survivor community underserved, yet at higher risk**
  - **Caregiver to brain injury survivor from 2010-2016**
  - **“A risk accepted by one is shared by all.”**

INTERNET SAFETY VS. INTERNET SECURITY

- **Disclaimer: These are entirely my definitions**
- **Internet Safety**
  - **Avoiding exploitation from online predators**
  - **Solutions are primarily non-technical (“Don’t give out personal information over the phone,”) but can be technical (blocking certain applications)**
- **Internet Security**
  - **Hardening the network from attacks over the Internet**
  - **Solutions are often technical (firewall rules), but can be non-technical (policies)**
- **This presentation will be mostly about safety**

THE RISK

- **Identity Theft**
- **Many people believe they have no information worth stealing – this is untrue**
  - **Personally Identifiable Information (PII)**
    - **Social Security numbers**
    - **Date of Birth/Marriage/Death**
  - **Protected Health Information (PHI)**
  - **Credit card numbers/bank account information**
  - **E-mail accounts (usernames and passwords)**
  - **Network access**
- **Fraudulent Tax Returns**

THE THREAT – SOCIAL ENGINEERING

- **Scam**
- **Many methods**
  - **E-mail (“Phishing”)**
  - **By phone (“Windows Help Desk,” “Internal Revenue Service”)**
  - **In person (“Survey taker,” “Shoulder surfing”)**
  - **Social media (“10 things you didn’t know about me”)**
- **Social engineer’s goal is to get victim talking**
- **Threat is becoming more sophisticated**

HOW DO SOCIAL ENGINEERS SUCCEED?

- **Trust or compliance**
  - **Appeal to authority (“IRS”)**
  - **(False) sense of urgency (“Windows Help Desk”)**
  - **Desire to help others (“Survey”)**
  - **Trusting our friends (Clicking on link in E-mail)**
- **Underestimation of the value of our own information**

QUESTION:

Which is more valuable on the black market: your Social Security number, your credit card number or your health record?

ANSWER

Social Security Number =

ANSWER

Social Security Number = $0.10

ANSWER

Social Security Number = $0.10

Credit Card Number =

ANSWER

Social Security Number = $0.10

Credit Card Number = $0.25

ANSWER

Social Security Number = $0.10

Credit Card Number = $0.25

Medical Record =

ANSWER

Social Security Number = $0.10

Credit Card Number = $0.25

Medical Record = (up to) $1,000.00

Source: **https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#22a674e850cf**

SOME OTHER USES FOR OUR INFORMATION

Source: Brian Krebs (www.krebsonsecurity.com)

- **Hacked PC**
  - **Spam "Zombie"**
  - **Distributed Denial of Service Attack**
  - **Stored credentials (used by attacker or sold)**
  - **Online gaming characters/goods/currency**
- **Hacked E-mail**
  - **Retail accounts (e.g., iTunes, Steam, Netflix)**
  - **Phishing source account**
  - **Work documents**
  - **Spam account**
  - **CEO fraud**

THE VULNERABILITY

- **Information Technology is becoming more common as a means to help survivors of Traumatic Brain Injury (TBI) and Acquired Brain Injury (ABI) with rehabilitation and daily life management**
- **TBI and ABI survivors are more vulnerable to social engineering attacks due to common cognitive impairments**
  - **Executive function**
  - **Deficits in attention**
  - **Memory deficits**

HOW WE CAN HELP

- **Healthcare Professionals**
  - **Be objective**
  - **Assess survivors' ability to understand and respond to the threat posed by social engineering**
  - **Inform caregivers of heightened risk**
  - **Point caregivers to sources of information for best practices in Internet safety and security**
  - **Educate caregivers as to best ways to mitigate their survivor's unique challenges**
- **Caregivers**
  - **Be supportive**
  - **Understand the threat**
  - **Model and reinforce best practices**

10 TIPS:

Keep your system up to date (“Auto Update”)

Use anti-virus programs

Don’t use free Wi-Fi for E-mail, banking or shopping

Be aware of your surroundings when using the internet in public

Don’t click on links in E-mail without verifying with sender

Don’t click on internet “pop-ups”

Don’t loan your smartphone to strangers

If you use public internet access (e.g., library), always log out of all websites and delete your browsing history

Never let an unsolicited caller “help” you with an internet problem or ask for your “help”

Never give out your username or password

EDUCATIONAL SOURCES

SANS Institute “Securing the Human” Project

- **OUCH! Newsletter (https://www.sans.org/security-awareness-training/ouch-newsletter)**

Verizon

- **Data Breach Investigations Report (DBIR) (http://www.verizonenterprise.com/verizon-insights-lab/dbir/)**

U.S. Department of Homeland Security

- **United States Computer Emergency Readiness Team (US-CERT) Tips (https://www.us-cert.gov/ncas/tips)**

QUESTIONS