Senior Citizens and Cybersecurity Awareness

Presenters/Co-authors:
Carlene Blackwood-Brown, M.Sc.
Yair Levy, Ph.D.
Steven Terrell, Ph.D.

College of Engineering and Computing
Nova Southeastern University
Overview

- Introduction
- Research Problem
- Attack Vector
- Users’ Actions Via Non-Secured Wi-Fi Networks
- Phishing Attacks
- Cybersecurity Awareness
- Research Significance
- Senior Citizens as Targets
- Research Questions
- Expected Impact of Research
Introduction

- Billions of dollars in losses accrued to Internet users due to cyber-attacks that exploit human vulnerabilities (Abawajy, 2014).
- Senior citizens are one of the most vulnerable groups of Internet users who are prone to cyber-attacks (Claar & Johnson, 2012; Grimes et al., 2010).
  - Reason: Limited awareness of cybersecurity countermeasures
Cyber Threats and Attacks

Captured between 4/10/2015 to 4/14/2015 for 24 sec
Cyber Crime Impact

THEME 1: SHOCKING SCALE: NUMBER OF VICTIMS

1 MILLION+ VICTIMS A DAY
EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES

50,000 VICTIMS EVERY HOUR
820 VICTIMS EVERY MINUTE
14 VICTIMS EVERY SECOND

Source: Norton cybercrime report

7/10 69%
69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime.

589 MILLION
Cybercrime has affected 589 million people in just 24 countries - equivalent to 9% of the entire population of the world.

65%
Among all cybercrime victims surveyed, nearly two thirds have fallen prey in the past 12 months alone - a total of 431 million adults in 24 countries.

431 MILLION
The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347 million) or Western Europe (400 million).
Cyber Crime Impact
Research Problem

The increase in the success of cyber-attack vectors due to limited awareness of cybersecurity countermeasures among Internet users.

Effects of Problem: Significant financial losses for governments, organizations, and the Internet users themselves (Abbasi et al., 2010; D’Arcy et al., 2009; Purkait et al., 2014).
Path through which a cyber-criminal can gain access to a network server or a computer in order to deliver a malicious effect or obtain information for malicious purposes (Lemoudden et al., 2013).

Non-secured wireless (Wi-Fi) networks, and phishing attacks are the most common ways for cyber penetrations to happen (Futcher, 2015; Noor & Hassan, 2013).

Prevention of personal identity information (PII) theft via access to non-secured networks, and preventing PII theft via email phishing identified among the top nine cybersecurity skills needed by non-IT professionals to counter cyber-attacks (Carlton & Levy, 2015).
**Users’ Actions Via Non-Secured Wi-Fi Networks**

- Non-secured Wi-Fi network settings: homes, libraries, malls, coffee shops, senior centers, etc. (Grimes et al., 2010)

- In 2013, a survey of 13,022 adults revealed the following about users’ actions on non-secured Wi-Fi networks (Symantec, Norton Report, 2013).

<table>
<thead>
<tr>
<th>Amount of Users</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>56%</td>
<td>Accessed social network account</td>
</tr>
<tr>
<td>54%</td>
<td>Accessed personal e-mail</td>
</tr>
<tr>
<td>29%</td>
<td>Accessed their bank account</td>
</tr>
<tr>
<td>29%</td>
<td>Shopped online</td>
</tr>
<tr>
<td>Three out of 10</td>
<td>Did not always log off after having used a public Wi-Fi connection</td>
</tr>
<tr>
<td>39%</td>
<td>Did not take any special steps to protect themselves when using public Wi-Fi networks</td>
</tr>
</tbody>
</table>
Phishing Attacks

- Online scams that use unsolicited messages to trick victims into revealing their financial and/or personal identity information (PII) to commit or facilitate other crimes such as fraud, identity theft and theft of sensitive information (Choo, 2011).

- Deception occurs because the messages seem like they are from legitimate organizations, especially banking and finance services.
2014 Phishing Attacks Statistics


- Represents a 20% increase over the two quarters of the same year.
Cybersecurity Awareness

- Involves informing Internet users of cybersecurity issues and threats, as well as enhancing their understanding of cyber threats so they can be fully committed to embracing security when they use the Internet (Rahim et al., 2015).

- Cybersecurity awareness countermeasures training focus on making Internet users more aware so that they can identify cyber-attacks as well as mitigate the effects of the cyber-attacks when they use the Internet (Rahim et al., 2015).
Research Significance

- To make senior citizens aware of the potential dangers of phishing attacks and using unsecured Wi-Fi networks, as well as how to mitigate the impacts of cyber-attacks.

- Senior citizens make up one of the fastest growing groups of Internet users (Iyer & Eastman, 2006).

- Internet Usage Statistics by Age (Perrin & Duggan, 2015).
  - Since 2012, more than half of all senior citizens report using the Internet.
    - Senior citizens have the greatest rate of change since 2000 among all age groups surveyed.
  - Cybersecurity awareness is essential for senior citizens as a countermeasure strategy to combat cyber-attacks (Choo, 2011).
Internet Usage: Young Adults vs Senior Citizens (2000 - 2015)

- **2000**
  - Young Adults: 70%
  - Senior Citizens: 14%

- **2015**
  - Young Adults: 96%
  - Senior Citizens: 58%
Senior Citizens as Targets

- One in five American senior citizen is a victim of online financial fraud, costing more than $2.6 billion per year (Willis, 2015).

- Senior citizens who are identity theft victims suffer devastating effects (Jones, 2001):
  - Loss of all their life savings
  - Feelings of shame for being victims
  - Decreased self-confidence
  - Exacerbated illnesses to include premature death
Are there significant mean differences in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training between a group of senior citizens who will receive cybersecurity awareness training and another group who will not receive cybersecurity awareness training over a period of six weeks?
Specific Research Questions

- Is there a significant mean difference in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training of senior citizens who will receive cybersecurity awareness training (Group A) before (t1) and immediately after (t3) the cybersecurity awareness training?

- Is there a significant mean difference in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training of senior citizens who will not receive cybersecurity awareness training (Group B) before (t1) and immediately after (t3) the other group receives the cybersecurity awareness training?

- Is there a significant mean difference in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training between a group of senior citizens who will receive cybersecurity awareness training and another group who will not, prior to the training (Group A vs. B @ t1)?
Are there significant mean differences in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training of senior citizens who will receive cybersecurity awareness training (Group A) over a period of six weeks following the training (t3, t4, t5, & t6)?

Are there significant mean differences in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training of senior citizens who will not receive cybersecurity awareness training (Group B) over a period of six weeks following the other group receiving the training (t3, t4, t5, & t6)?

Are there significant mean differences in the levels of cybersecurity awareness, self-confidence, and perceived risk of identity theft, as well as intrinsic motivation and extrinsic motivation to pursue additional cybersecurity awareness training between a group of senior citizens who will receive cybersecurity awareness training and another group who will not, over a period of six weeks following the training (Group A vs. B @ t3, t4, t5, & t6)?
Proposed Measurements and Times for Group A (group that will receive the training) and Group B (group that will not receive the training)

<table>
<thead>
<tr>
<th>Time (t)</th>
<th>t₁</th>
<th>t₂</th>
<th>t₃</th>
<th>t₄</th>
<th>t₅</th>
<th>t₆</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure</td>
<td>MA₁(a, b, c, d, &amp; e)₁</td>
<td>MA₂(a, b, c, d, &amp; e)₂</td>
<td>MA₃(a, b, c, d, &amp; e)₃</td>
<td>MA₄(a, b, c, d, &amp; e)₄</td>
<td>MA₅(a, b, c, d, &amp; e)₅</td>
<td>MA₆(a, b, c, d, &amp; e)₆</td>
</tr>
<tr>
<td>Treatment</td>
<td>Tₓ</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Key**
- t₁ = Before treatment; t₃ = Immediately after; t₄ = Two weeks after; t₅ = Four weeks after; t₆ = Six weeks after
- a = Cybersecurity Awareness; b = Self Confidence; c = Perceived Risk of Identity Theft; d = Intrinsic Motivation; e = Extrinsic Motivation
- MA₁, MA₂, MA₃, MA₄, MA₅, MA₆ = Measure Group A at time 1, 3, 4, 5 & 6
- MB₁, MB₂, MB₃, MB₄, MB₅, MB₆ = Measure Group B at time 1, 3, 4, 5 & 6
Expected Impacts of Research

- To reduce the success of cyber-attacks vectors that result from limited awareness of cybersecurity countermeasures among senior citizens
- To increase the awareness levels amongst senior citizens regarding issues of cybersecurity
- To motivate senior citizens to seek training in cybersecurity countermeasures
- To establish how increased awareness of cybersecurity countermeasures can mitigate the impacts of cyber-attacks amongst senior citizens
- To show how increasing cybersecurity awareness among senior citizens can positively contribute to aging
Questions?

"Okay your father managed to get a mouse. Now how do we use it?"
Thank You


References


