NSU NOVA SOUTHEASTERN UNIVERSITY

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

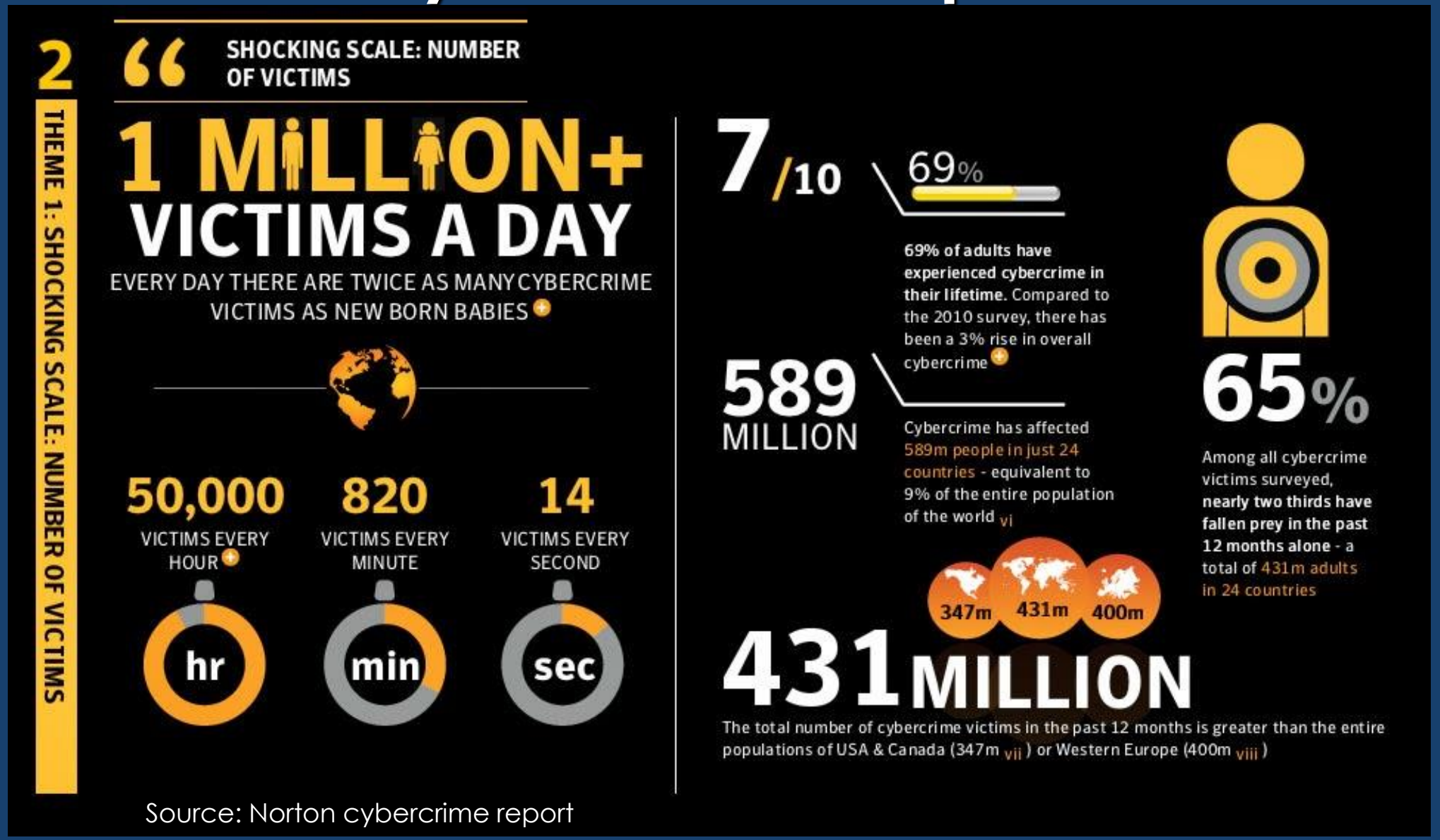
Introduction

- 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



Source: Norton cybercrime report

http://mobileadvertisingwatch.com/wp-content/uploads/2015/09/Gartner-The-Internet-Of-Things-Will-Change-Cybersecurity-Forever.jpg

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).

Attack Vector

- 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).

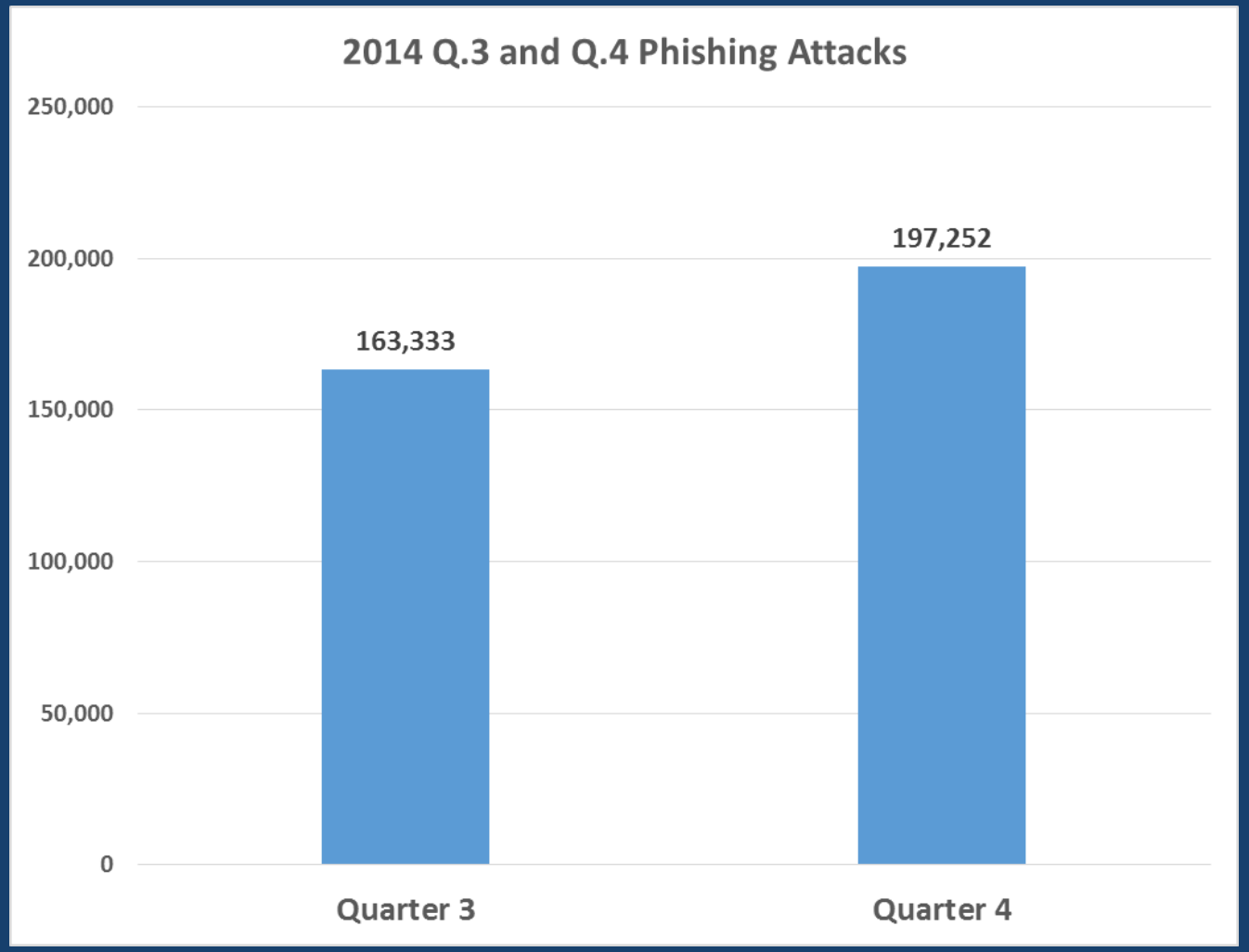
Amount of Users	Actions
56%	Accessed social network account
54%	Accessed personal e-mail
29%	Accessed their bank account
29%	Shopped online
Three out of 10	Did not always log off after having used a public Wi-Fi connection
39%	Did not take any special steps to protect themselves when using public Wi-Fi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

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

- Statistics (Anti-Phishing Working Group, 2015).



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

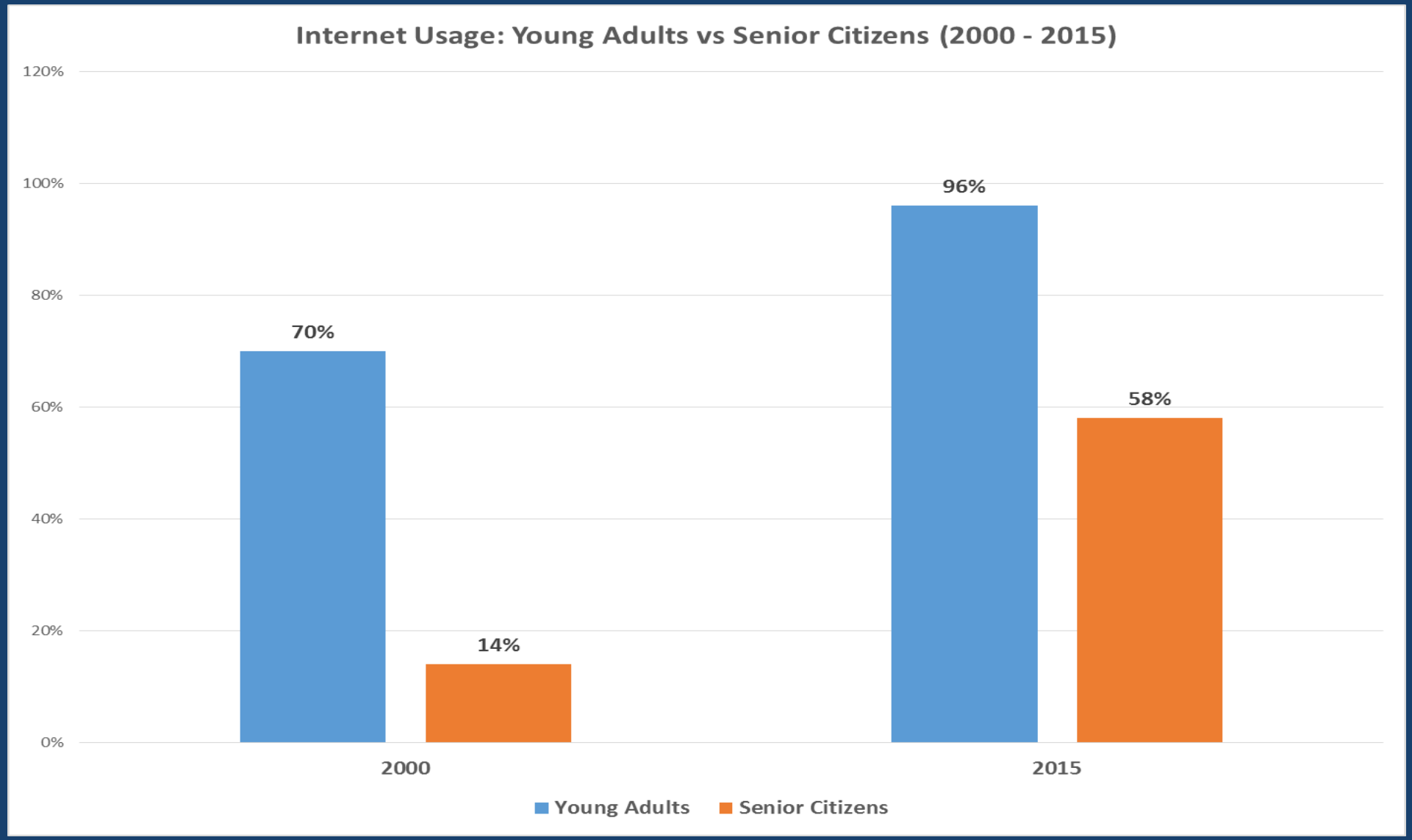
Cybersecurity Awareness

- 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).

Research Significance (Cont.)



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

Main Research Question

- 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)?

Specific Research Questions (Cont.)

- 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)

Time (t) ⟶

	t_1	t_2	t_3	t_4	t_5	t_6
	Measure	Treatment	Measure	Measure	Measure	Measure
Group A (The Experimental Group)	$M_A(a, b, c, d, \& e)_{t_1}$	T_x	$M_A(a, b, c, d, \& e)_{t_3}$	$M_A(a, b, c, d, \& e)_{t_4}$	$M_A(a, b, c, d, \& e)_{t_5}$	$M_A(a, b, c, d, \& e)_{t_6}$
Group B (The Control Group)	$M_B(a, b, c, d \& e)_{t_1}$	No	$M_B(a, b, c, d \& e)_{t_3}$	$M_B(a, b, c, d \& e)_{t_4}$	$M_B(a, b, c, d \& e)_{t_5}$	$M_B(a, b, c, d \& e)_{t_6}$

Key

t_1 = Before treatment; **t_3** = Immediately after; **t_4** = Two weeks after; **t_5** = Four weeks after; **t_6** = Six weeks after

a = Cybersecurity Awareness; **b** = Self Confidence; **c** = Perceived Risk of Identity Theft; **d** = Intrinsic Motivation; **e** = Extrinsic Motivation

$M_{A_{t_1}}$; $M_{A_{t_3}}$; $M_{A_{t_4}}$; $M_{A_{t_5}}$; $M_{A_{t_6}}$ = Measure Group A at time 1, 3, 4, 5 & 6

$M_{B_{t_1}}$; $M_{B_{t_3}}$; $M_{B_{t_4}}$; $M_{B_{t_5}}$; $M_{B_{t_6}}$ = 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 ctizens can positively contribute to aging

Questions?


www.zeebarf.com
zeebarf00
"Okay your father
managed to get a mouse.
Now how do we use it?"


These social medias are great, Harold! They make it so much easier to complain about young people these days.
AGENT-X COMICS
WWW.AGENT-X.COM.AU

Thank You

References

- Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behavior & Information Technology, 33*(3), 236-247.
- Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly*, *34*(3), 435-461.
- Anti-Phishing Working Group (2015). Phishing activity trends report, 4th quarter 2014. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf
- Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the 2015 IEEE SoutheastCon,* Ft. Lauderdale, Florida, pp.1-6.
- Choo, K-K., R. (2011). The cyber threat landscape: Challenges and future research directions, *Computers & Security, 30*(8), 719-731.
- Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29.
- D' Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.
- Futcher, A. L. L. (2015). A framework to assist email users in the identification of phishing attacks. *Information & Computer Security, 23*(4), 1-14.
- Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology, 36*(3), 173-192.

References

- Iyer, R., & Eastman, J. K. (2006). The elderly and their attitudes toward the Internet: The impact on Internet use, purchase, and comparison shopping. *Journal of Marketing Theory and Practice, 14*(1), 57-67.
- Jones, T. L. (2001). Protecting the elderly. *Law & Order, 49*(4), 102-106.
- Lemoudden, M., Bouazza, N. B., El Ouahidi, B., & Bourget, D. (2013). A survey of cloud computing security overview of attack vectors and defense mechanisms. *Journal of Theoretical & Applied Information Technology*, *54*(2), 325-330.
- Perrin, P., & Duggan, M. (2015). *Americans' Internet Access: 2000-2015. Pew Research Center*. Retrieved from http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/
- Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security, 22*(3), 194-234.
- Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes, 44*(4), 606-622.
- Shillair, R., Cotten, S. R., Tsai, H-Y. S., Alhabash, S. LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48,* 199-207.
- Symantec Corporation. (2013). *2013 Norton Report*. Retrieved from http://www.symantec.com/en/ca/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
- Willis, D. P. (2015, June 15). 5 steps for seniors to avoid financial fraud. *McClatchy - Tribune Business News* Retrieved from http://www.app.com/story/money/business/consumer/2015/06/15/senior-financial-fraud/71264182/