Project Proposal

The problem:

There has been an explosion of technology. In 2013, mobile device internet usage overtook personal computers and laptop usage for internet searching. There are now more mobile devices in the world than there are people (Connected, 2015) – and this does not include personal computers or laptops. With the rise of technology, there has also been a rise of security threats. According to Mike Miliard from Healthcare IT News, IT departments are 'scrambling' to deal with these [cloud and bring your own device] technologies, which are developing at a 'whirlwind' pace" (2013). Technology is everywhere; security threats are everywhere.

Technology users are included in the list of security threats. In fact, according to Chuck Romano, one of our biggest threats to IT security is social engineering (2011). Marcel Brown, owner of Marcel Brown Technology Services, in his article entitled, "Computer Scams Are Everywhere!" speaks about the tremendous increase in reported scams the company is receiving from clients. These scammers gain access to a user's computer using scare techniques, and then hold the computer hostage (2015).

What is it that makes people so trusting and gullible? Perhaps part of the problem is the many myths and misconceptions concerning information security. People believe that they would never be a target (Wilson 2016). Yet everywhere someone turns, there is another lurking computer security scam. Investigating more into common misconceptions, Security Specialist Ken Wilson comments on several additional myths and misconceptions - people believe that being behind a firewall or protecting WiFi will keep them secure. Many of the same security myths in Wilson's article are repeats from Fahmida Rashid's article on the "Security Top 10 Security Myths". The bottom line here is that myths and misconceptions regarding computer security influence making informed decisions, which puts everyone at risk.

In part of the research on this topic, free security courses through massive open online courses (MOOCs) from FutureLearn, EdX, Coursera, and Udemy were reviewed for availability, engagement, and content. Courses contained video, articles, and low-level quizzes. However, the courses were not engaging, and there was no opportunity for students to interactively learn the content. There are many non-MOOC security courses that do exist, many of the courses are not geared for the everyday device user – many courses are offered for people in the computer security workforce, a level too high for the everyday user. Andra Zaharia writes in her blog, "There are just not enough cyber security courses for beginners out there! When you want to learn in a very organized manner, you need more than articles and shallow information" (2017).

A good general computer security course geared towards the everyday user is needed. The course needs to be interactive and engaging. In Sara Briggs's article, "The Science of Attention…", hits on several key points on learning. There is not a problem with technology. It is not a distraction. Education needs to be changed to accommodate how students learn (2014). Courses that are not interactive and engaging make it difficult to pay attention, process information, and retain learning. In order for this course to be successful and have an impact, it is extremely important that learning is retained so that it can be applied to life situations.

In summary, general computer security knowledge for the everyday technology user is a huge problem, especially since there are security risks everywhere. Courses that exist are either not engaging or too high level for the everyday user.

The Solution / Course Content:

To address the gap in the general computer security knowledge for the everyday technology user, a broad-spectrum security class will be created. This course will include, but not be limited to, the following topics:

1. **Internet basics.** People are internet addicts. Life for some revolve completely around the internet. There are many myths, including "It won't happen to me" (Rashid, 2013) and "Phishing is primarily limited to emails" (Looking Glass, 2016). People need to be educated to recognize how they are a target and recognize when something is a scam. They need to understand risks so that they could minimize potential damage. This section on internet basics would include information regarding free WiFi, phishing scams, social engineering scams.
2. **Malware basics.** This topic is very important as users are constantly exposed. According to an article by Darren Paili, there are 227,747 new malware samples released daily (2014). That's over 80 million per year. Yet a common belief is the only way to get infected is by doing something risky (Wilson, 2016). Everyone is constantly exposed and needs to be aware of malware.
3. **Passwords and authentication.** With people having so many different accounts, it is very tempting for people to always use the same username and password if possible. This is very troublesome, as breaches seem to be a common theme these days. Robert Lemos in his article about the LivingSocial Database breach writes, "LivingSocial forced every user to change their password, but previous data breaches have shown that a majority of people reuse passwords across sites, threatening their accounts on other Web services and even their employer's network" (2013). Even if there isn't a breach, a common myth is that credentials by large companies are secure. But according to Brent Jensen's article on myths of password security, over half of companies store passwords in plain text (2016). Employees of the company can gain access to a user's credentials. It's a scary thought that once a hacker or employee has the person's account and username for one site, the hacker or employee also has the person's credentials for all other sites that are used, including potentially VPN access to the person's employer. It is important for everyday users to understand passwords and authentication, how to choose passwords, and how to safeguard them.
4. **Encryption/Cryptography**. A favorite myth is that if data is encrypted, it's safe. But people do not understand that there are different encryption methods. Data at rest or in transmission might not both be encrypted. "Channel encryption is only a portion of the protection your sensitive data needs" (Oliver). General users do not understand that encryption is not very helpful if a person can gain access directly to the device using credentials.

Tools:

- Articulate Storyline will be used to build out the interactive course
- Adobe Photoshop will also be used to build images as needed
- Articulate 360 will be used to host the course for this class, with the ultimate goal that once this course is completed, it will be hosted by an MOOC.
- The course will also be able to be ran entirely off-line. This course will be also placed in a drop box as a backup method of accessing the course.

Course Outline:

1. Internet Basics
    a. Internet myths/history/real life examples
    b. Internet dangers
    c. Social engineering
    d. Recognizing scams
    e. Interactive Activity
2. Malware
    a. Malware myths/history/real life examples
    b. Types of malware
    c. Protecting against malware
    d. Interactive Activity
3. Passwords and Authentication
    a. Password myths/history/real life examples
    b. Strong passwords
    c. Keeping passwords safe
    d. Interactive Activity
4. Encryption/Cryptography
    a. Internet myths/history/real life examples
    b. Encryption basics
    c. Interactive Activity

Nature of the Development / Course Structure:

The broad-spectrum security course should also include real-life examples and history, not only information on massive attacks, but also information on common schemes and challenges that the user may face. Each topic or module should start by introducing a myth, providing relevant history, providing information about the topic (this could be video, readings, lecture) in an interactive way, and then hands-on practice/simulation or a hands-on simulation. Content needs to be interactive and engaging; the course will contain text and interactive examples. Low-level comprehension checks should be kept at a minimum, and should not be the sole source of assessment. Furthermore, this course should be flexible to accommodate multiple devices and platforms, and not require teacher interaction. Users should be able to go through the course independently. After all, student participation tends to decline over time for MOOCs (Nadeem, 2013).

Milestone 1 deliverable:
Due by July 2nd, 2017, milestone 1 will include high-level lesson plan and materials for the entire course. Interactive activities will have a basic outline, but might not be finalized. A draft build of Internet Basics will also be designed and published for review.

Milestone 2 deliverable:
Due by July 16th, 2017, milestone 2 will include a refined version of Internet Basics. Malware and Passwords will have a draft built and published for review.

Task list (complete by):

- 6/10/17 COMPLETED Research/evaluation on current MOOC security courses
- 6/17/17 COMPLETED Basic course outline / extended research
- 6/23/17 Refine high-level course plan
- 6/25/17 Weekly Status Report 1
- 7/1/17 Draft of Internet Basics
- 7/2/17 Milestone 1: Publish Draft of Course / High-level plan (Weekly Status Report 2?)
- 7/8/17 Draft of Malware
- 7/9/17 Weekly Status Report 3
- 7/9/17 Review and incorporate peer feedback
- 7/15/17 Draft of Passwords
- 7/15/17 Refinement of Internet Basics
- 7/16/17 Milestone 2: Publish Draft of Course (Weekly Status Report 4)
- 7/19/17 Draft of Encryption
- 7/23/17 Weekly Status Report 5
- 7/23/17 Review and incorporate peer feedback
- 7/23/17 Draft of Project Paper
- 7/27/17 Draft of Project Presentation
- 7/30/17 Refinement of Project, Paper, Presentation
- 7/31/17 Final Project
- 7/31/17 Project Paper
- 7/31/17 Project Presentation

Bibliography

Briggs, S. (2014, June 28). The Science of Attention: How To Capture And Hold The Attention of Easily Distracted Students. Retrieved June 15, 2017, from http://www.opencolleges.edu.au/informed/features/30-tricks-for-capturing-students-attention/

Brown, M. (2015, June 01). Computer Scams Are Everywhere! Retrieved June 12, 2017, from http://marcelbrown.com/2015/05/17/computer-scams-are-everywhere/

Connected. (2015, August 03). More mobile devices in the world than people – how many do you have? Retrieved June 10, 2017, from https://www.connected-uk.com/more-mobile-devices-in-the-world-than-people-how-many-do-you-have/

DeVry University MOOC. (n.d.). Cyber Security. Retrieved June 5, 2017, from https://www.udemy.com/cyber-security/learn/v4/overview

Jensen, B. (2016, October 31). 5 Myths of Password Security. Retrieved June 14, 2017, from https://stormpath.com/blog/5-myths-password-security

Lemos, R. (2013, April 30). Password Reuse Remains a Danger After LivingSocial Database Breach. Retrieved June 17, 2017, from http://www.eweek.com/security/password-reuse-remains-a-danger-after-livingsocial-database-breach

Looking Glass. (2016, April 14). Top Five Phishing Myths Debunked. Retrieved June 16, 2017, from https://www.lookingglasscyber.com/blog/threat-reports/phishing/top-five-phishing-myths-debunked/

Miliard, M. (2013, December 04). Security risks on the rise for 2014. Retrieved June 13, 2017, from http://www.healthcareitnews.com/news/security-risks-rise-2014

Nadeen, M. (2013, December 25). Research: Student Participation Declines Dramatically in MOOCs. Retrieved June 17, 2017, from http://www.educationnews.org/online-schools/student-participation-decline-dramatically-in-mooc/

Oliver, R. (n.d.). 8 Myths of Computer Security. Retrieved June 17, 2017, from http://www.tech-mavens.com/myths.htm

The Open University, F. (n.d.). Introduction to Cyber Security - Online Course. Retrieved June 04, 2017, from https://www.futurelearn.com/courses/introduction-to-cyber-security/

Pauli, D. (2014, November 06). 158 new malware created EVERY MINUTE. Retrieved June 16, 2017, from https://www.theregister.co.uk/2014/11/06/158_new_malware_born_every_minute/

Rashid, F. (2013, June 13). Security Top 10 Security Myths: Misconceptions and Exaggerations About Threats and Technologies. Retrieved May 27, 2017, from http://www.securityweek.com/top-10-security-myths-misconceptions-and-exaggerations-about-threats-and-technologies

Romano, Chuck (2011, November 1). The Social Engineering Threat to IT Security. Retrieved May 23, 2017, from https://www.technibble.com/the-social-engineering-threat-to-it-security/

The University of Adelaide. (2016, August 22). Cyberwar, Surveillance and Security. Retrieved June 04, 2017, from https://www.edx.org/course/cyberwar-surveillance-security-adelaidex-cyber101x-0

Universiteit Leiden. (n.d.). Security & Safety Challenges in a Globalized World. Retrieved June 6, 2017, from https://www.coursera.org/learn/security-safety-globalized-world/home/welcome

Wilson, K. (2016, December 9). 6 Common Misconceptions About Computer Security. Retrieved May 27, 2017, from https://bdtechtalks.com/2016/12/09/6-common-misconceptions-about-computer-security/

Zaharia, A. (2016, May 17). 50 Useful Cyber Security Online Courses You should Explore. Retrieved May 27, 2017, from https://heimdalsecurity.com/blog/50-cyber-security-online-courses-you-shouldknow-about/