Aloha and welcome! Good afternoon for many of you and good evening for some of you! My name is Adam Tanare Jr. I am a third year graduate student in Educational Technology M.Ed. Program at the University of Hawai‘i at Manoa. I hope to receive my degree at the conclusion of this semester! My educational area of interest, and coincidentally, my lifelong hobby, is video games. My project is titled “Computer Security Strategies”, an Instructional Design Approach. In this project, I created a set of small computer games for my participants to play!

I don’t have a twitter or facebook account, so if you want to contact me, please feel free to send me an email, or post a comment on my TCC page!
So, in a nutshell, what is my project about? Yes, it is about computer security strategies. But, at it’s core, it is a:

Instructional design module. Like many of my colleagues and classmates, I created a module with the purpose of imparting information and knowledge. We create such a module as “instructional designers”, whose job consists of evaluating available information that will best aid in developing effective instructional tools.

It is completely web-based! If you would like, you can access the module anytime after this presentation by visiting:
http://computersecuritystrategies.weebly.com/

Lastly, it is a “hybrid”, meaning it is a mix of at least two things. What do I mean by “hybrid” in this context?
The web-based module is comprised of both text and computer game!

The text portion of the module are instructional strategies that utilized paragraphs and images to teach the audience computer security.

The computer game portions of the web-based module are interspersed in-between different sections, and serve as the embedded test portion.

An embedded test is anything that allows participants in a learning module to practice what they have learned.

Now that we’ve established that my computer security module is a unique mix of text and game, let’s poll the audience!
Which of these categories do you consider the most popular gaming platform today?

Please select A for video game consoles like the Playstation 3 and Xbox360

Or B for computer gaming

Or C for mobile gaming, which includes handheld platforms, tablets, and phones.

RESULTS: Ah, it looks like......

I asked you all this question because my preconceptions of what I thought today’s generation of kid’s like in a video game are different from what they actually like. I based my conceptions on what I liked as a kid, which were console games with games such as Mario, Final Fantasy, and Street Fighter. With the introduction and proliferation of mobile gaming, particularly tablet and phone gaming, the video game market has seen a monumental shift, and so has its demographics. This played a huge role in my development process, as I will talk about more later on.

You know, perhaps the preferences of gaming platform differ depending on country of origin? Let’s take another poll of where we are in the world, shall we?
I apologize. My computer has really been acting up lately, and it seems my world map image got corrupted. Anyways, please place a dot on where you are logging in from in the world today.

Results: Ah, it looks like a lot of you are logging in from .....
Moving right along into today’s presentation, I will be covering:

The research that helped shape the development of my module.

The processes I took during the development of the project module.

The trials and tribulations of my implementation, revision, and re-implementation phase,

And finally, the results and discussion of results.
First off, an instructional designer would not start to develop a product unless first identifying a need for said product. For my project, I identified an instructional need for more knowledge of cyber security. Cyber-attacks have become more frequent, and are much more visible and publicized in the media. General users are either unaware of dangers or are apathetic about risks.

Last year, in 2011, a large number of cyber-attacks were reported on.
As you can see in this word cloud, quite a small number of large organizations were hit.

Gaming entities like Nintendo and Bethesda, a game development company, were hit.

Defense contractor Lockheed Martin also fell victim.

Governments such as Turkey and Spain were affected to some capacity.

Financial megacomglomerates like Visa and Master Card fell victim as well.

Even the FBI and CIA were not safe from the likes of hacker groups such as Anonymous and LulzSec.
Many attacks similar or more simpler than the ones I just discussed, aim to collect thousands of user account information. User account information typically includes a username, associated email, and passwords. Accounts that involve financial transactions will also ask for your personal information and financial information to be kept on file.

While it may seem obvious that having personal and financial information compromised is a huge threat to individuals, some individuals may even exacerbate the threat by simply reusing the same username, email, and passwords for all their other accounts. Compromised information from one account can thus can be used to exploit other account owned by victims.
While I try to be as safe as possible with my information online, it wasn’t until a major attack on Sony’s Playstation Network last April that I really wanted to learn more about cyber security. Can you all guess how many accounts were compromised in that attack?

77 hundred?
77 thousand?
77 million?
77 billion?

Results: Yes, 77 million accounts being compromised is insane isn’t it? In fact, this has affected me personally because I am one of those 77 million affected accounts! Luckily, I did not have any credit card information on file, so the only steps I had to take was to change my login information.
Other computer security concepts that I researched regarded software updating. General users typically neglect the practice and think of it as cumbersome or intrusive. What they may not know is that the software updates are meant to fix vulnerabilities in their computer software. With a gap in time between when a user has outdated software, to when they update all their software, if at all, is a timeframe that hackers take advantage of. Malicious code written by hackers look to exploit these unpatched vulnerabilities, in many oft-used software, like Java, Flash, Quicktime, and Microsoft.Net framework.
Lastly, online security is also just as important as personal computer security. There are many malicious links that are online, which are designed by hackers to direct you to a malicious website, legit looking or not. These sites then attempt to load malicious things onto your computer to infect it. It’s a social engineering attempt; hackers try to get you to click on something you shouldn’t but you may click it because it either looks harmless or to enticing to pass up.
These types of social engineering attacks can be very harmful because they can harm your computer in some way. In this screenshot, the user’s antivirus software luckily intervened.

Of note, some social engineering attacks are not meant to be harmful at all.

Many can be harmless pranks meant to make you feel a variety of emotions.

One that I fell for recently was a YouTube video announcing the “Sega Dreamcast 2” video game console. I was so excited about it!
But then clicking on that link led me to a music video with Rick Astley singing his 1987 #1 hit single “Never Gonna Give You Up”. Yes, internet memes such as this one can be considered a social engineering attack, as you were socially engineered into doing it!
Moving on to the project development, it started in August 2011, at the start of my final year in the ETEC program. I had spent the summer researching a lot of cyber security topics as a reaction to the major PSN attack of the prior April. I felt that strong password practices were vital to EVERYONE, and I myself started making very complicated passwords. I wanted to teach others the importance of strong passwords and how to make them.
I had this conception that computer security is too complicated or time consuming a topic to learn or practice. At least from my observations. So, with my personal interest in video games, I thought I could create a video game to help teach the topic of computer security.
Originally, the audience was going to be adults. They would obviously have much more important accounts to secure like banking, credit cards, etc. However, with the advise and help from classmates, and the help of an advisor, I was able to change to a younger audience.
So adults were eliminated from the equation, and now my focus was with 6th, 7th, and 8th graders. However, shortly before the time of implementation, a school administrator I was working with said that she could only get the 6th grade to work with me.
Thus, the purpose of the project became to create an instructional design module that would make the task of teaching basic computer security concepts more engaging and relevant to children.
Keller’s ARCS model of Attention, Relevance, Confidence, and Satisfaction was used to guide my development.

I intended my hybrid module to:

Gain the attention of the audience by kind letting them know of the dangers that are out there in the computer world.

It also was a relevant topic to them because they all had different accounts to login to, and all of them had gmail accounts.

I had hoped they would gain confidence to protect against threats by learning defensive procedures from my module.

I utilized a hierarchy chart to guide my initial development.

And lastly, the students would be satisfied with playing a video game rather than a
typical lesson.
This is what it looked like before I had worked with the students. Crazy, huh? After working closely with some of the students during two pilot study sessions, and from great advice from classmates, I had no choice but to narrow down my scope.
This is what was left of my hierarchy chart. I ended up working with the following topics, split into two sections, or chunks:

Section 1: Computer Security
This included passwords, keyloggers and software updating

Section 2: Online security
This SSL and HTTPS security, and SEO poisoning.
I created my module with Weebly.com, a free website creation tool. I used it because it had drag and drop functionality, and it was simple to use. I had used it in many previous class assignments and so I was already fairly familiar with its interface.
For the computer games I developed, I used YoYo Game’s GameMaker: HTML5 software. I purchased a single use license for $99. I was actually much more proficient with another software called RPG Maker, but because it was Windows only, I chose HTML5 because it could port games to the web.

It also featured simple drag and drop interface, and could create simple 2d games. I spent 1½ months learning this software on my own by studying youtube videos, reading through 2 official tutorial books, and other online text-based tutorials.
With the help of my advisor and the Dean of Curriculum at my target audience school, I was able to secure two dates to conduct pilot studies with select 6th graders. I was able to work with 8 students during the 1st pilot study on February 7th, 2012. I made as many changes as I could based on feedback before going into the 2nd pilot study on Feb. 9th, also with 8 students. The pilot studies were really more of a focus group, as I was able to communicate directly with the students as they did the module. I also asked them to time themselves on major sections. More about this can be read in my paper.

Finally, after the 2nd pilot study, I frantically made many revisions to the website and the video games. In fact, the save file for my game projects became corrupted, and I had no choice to build the game from the ground up after the 2nd pilot study!

Feb 16th quickly came around, and I was happy that I was able to rebuild my game more faster than I did originally, and I had made drastic revisions, mostly reductions, to the website. This included cutting out a ton of text, and putting nice kid friendly pictures all over the site.
Student’s progressed through the module in the following order:
The computer games were designed to be simple maze levels where they had to navigate a character safely to the exit. The levels were as follows:

Load screens were screens where players could read about how to play the game, or information about a learning objective.

Maze levels were as described earlier.

Quiz rooms were rooms where players had to answer the question correctly in order to advance. Load screens prior to quiz rooms always contained the right answer.
Here is a screenshot of the front page of the module. You can see a lesson overview at the bottom. While I don’t have screenshots for you of previous revisions, I can assure you that there is a night and day difference between the them. I used a light sky background which looked more welcoming, and used free images provided by weebly’s search feature. Navigation was limited to NEXT or PREVIOUS buttons at the bottom of each page.
Here is a screenshot of the computer games. Players controlled THAT little blue man which I named SPADE for STRONG PASSWORD AUGMENTOR DEFENSE ENGERGIZER MAN. Players had to collect all password powerups to advance to the exit, which was blocked by a malicious object such as a virus, malware, trojan horse, worm, or keylogger. I made the password powerups look like numbers, symbols, characters, upper and lowercase letters, to reinforce the concept of using lots of these in a password. A scoring mechanism was also present, where players gained points for collecting powerups, but lost points gradually as long as they stayed in the level. They could step on this little information icons to freeze the dropping score and read important tips for the game or the module; however no matter what I tried, not many students read these things.
Here is a screenshot of the quiz room. Players had to move spade over the correct answer’s slot to continue. To discourage players from randomly choosing answers so they could continue, players would gain a large 1000 points for a correct answer, but would lose 1000 points for every answer they got wrong. From what I observed, most students earnestly tried their best to avoid losing points, and that had the intended effect I wanted.
After removing participants who were also present in the pilot study, the valid set had 22 participants.

<table>
<thead>
<tr>
<th>Section 1</th>
<th>Pre-Test</th>
<th>Post-Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Brute Force Attack</td>
<td>41%</td>
<td>86%</td>
</tr>
<tr>
<td>2. Password Strength</td>
<td>64%</td>
<td>77%</td>
</tr>
<tr>
<td>3. Keyloggers</td>
<td>18%</td>
<td>77%</td>
</tr>
<tr>
<td>4. PW memorization</td>
<td>45%</td>
<td>86%</td>
</tr>
<tr>
<td>5. PW makeup</td>
<td>73%</td>
<td>100%</td>
</tr>
<tr>
<td>6. Software updates</td>
<td>23%</td>
<td>32%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section 2</th>
<th>Pre-Test</th>
<th>Post-Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. SSL: Secure Socket Layer</td>
<td>45%</td>
<td>64%</td>
</tr>
<tr>
<td>8. HTTPS: Hypertext Transfer Protocol Secure</td>
<td>50%</td>
<td>27%</td>
</tr>
<tr>
<td>9. Purpose of SSL &amp; HTTPS</td>
<td>5%</td>
<td>23%</td>
</tr>
<tr>
<td>10. Location of security information in browser(s)</td>
<td>5%</td>
<td>0%</td>
</tr>
<tr>
<td>11. SEO: Search Engine Optimization</td>
<td>77%</td>
<td>86%</td>
</tr>
<tr>
<td>12. Revealing Hyperlink Address</td>
<td>14%</td>
<td>73%</td>
</tr>
</tbody>
</table>
Discussion

- Students really enjoyed the module
- Average to above average improvement from pre-test to post-test for many of the 12 questions
- Pilot study sessions were instrumental in improving module success
Many of the feedbacks, verbal or though survey, yielded from the pilot studies were implemented into the small group evaluation.
Open-Ended Feedback

Overall
- I liked that it was very educational and not very boring, like most educational games.
- I liked it when I was doing all the solving and the part we had to go through the room

Mechanics
- The part of the video game that I liked was when you collect the lock and you become invincible, you can kill the bad stuffs and get more points.
- How the bad things catch you quickly.
- Dying from the black stuff and the pink circles
Conclusion

- Entirety of experience is very valuable
- Reflection: Do a better audience analysis
- Be more flexible
- Possibility for longitudinal study, or an improved study in the future
- Commercial application?
Thank you! Questions?

tanare@hawaii.edu
Credits

All visual images used were from:

- Microsoft PowerPoint 2010 clip art
- Google Images using the following filter criteria:
  - Advanced search
  - Usage rights:
    - Free to use, share, or modify