Portfolio Project

EDUC 765: Trends and Issues in Instructional Design

By: [Anne Carlsen]

Submitted [June 20, 2021]

Project Proposal

CYBER SAFETY

SPONSORING ORGANIZATION

Virtue Systems, LLC.

Virtue Systems is a two-person company that provides IT support services primarily to property management companies in the Phoenix metro area. Their mission is Technology, Simplified.

PROJECT DESCRIPTION

Senior citizens periodically contact the busy owner for consultation and computer troubleshooting, but often could answer their questions with basic internet searches. Many times, these consultations do not result in additional revenue, but the company still strives to help those who ask. Recently the company began building a social media campaign that promotes cyber awareness to mitigate some of the problems many senior internet users commonly face with emerging technology. Virtue Systems wants to expand this campaign with an easy-to-use cyber safety training module for the company website. The proposed training will cover Social Media Privacy, E-Commerce, Passwords, Wi-Fi Security, and Scams.

AIM

Provide free of charge cyber safety training module for senior citizens accessing virtuesystems.net to promote the company while limiting unnecessary pro bono services.

TARGET AUDIENCE

- Senior Citizen internet users who are unfamiliar with the medium
- Website visitors that are unfamiliar with the internet medium

DELIVERY OPTIONS

This instruction will be delivered as asynchronous computer-based training (CBT) available on the company website. When customers view the website for help, they can find and access the CBT without the need for a phone call to the owner.

Front-End Analysis: Instructional Need

INSTRUCTIONAL NEED

Before moving forward, there must be a determination that instruction is the answer to this problem. A conducted needs assessment shows two perspectives of the problem: the IT organization, and the senior citizen client. An interview with the owner of Virtue Systems illustrates that it is an existing performance problem because the organization struggles with time management when it provides pro-bono consultations to seniors that do not fully understand how to safely use internet technologies, but that is only part of the picture.

These clients show a critical incident need by the increase in inquiries from victims of cyber safety incidents such as downloaded malware and password theft. It is not fair to assume that all seniors lack this knowledge, so it is important to analyze those in the same demographic that are more tech-savvy to identify the gap in desired behavior and determine if instruction is the ultimate method used to solve the problem.

There is a universally understood gap between seniors that have kept up with internet changes and those that have not. Seniors that are cyber-savvy are less vulnerable to scams and fraud as they have learned to identify risks through experience and shared knowledge. Less cyber-savvy seniors are not exposed to these risks until they access internet technology and are unprepared to mitigate them as they are uninformed of the potential dangers. The main difference between these two groups is how much exposure they have had to gain cyber safety knowledge.

The goal of this project frees up Virtue Systems' valuable time by raising the level of cyber safety knowledge in the less savvy senior to the point where they are aware of risks and less vulnerable like their savvy counterparts. There are only two methods of gaining this knowledge: through experience or through instruction. As experience can take years to build, a reasonable conclusion shows instruction is the practical alternative as it illustrates the critical risks in a concise lesson.

Front-End Analysis: Learner Characteristics

LEARNER ANALYSIS

Primary Audience

- Senior Citizens desiring cyber safety training

Secondary Audience

- Other internet users desiring cyber safety training

General Learner Characteristics

- Adult learners age 55+, age is not a requisite, but that is the target audience
- Gender and socioeconomic status are irrelevant to training as long as learners have access to a computer and internet technology

- Basic level users of computer and internet technology
- English Speaking, unless learners have access to translators or translating devices

Entry Characteristics

- Basic Computer and Operating System manipulation skills
- Basic Internet Browser manipulation skills
- Basic Smartphone manipulation skills (beneficial, but optional)

CONTEXTUAL ANALYSIS

Orienting Context

- Learners that take the training have a goal of gaining cyber safety skills and knowledge.
- Learners will find this training useful both as a preventative step they can take to mitigate the need for consultation and becoming less vulnerable online.
- As the training is a CBT and not graded, the learner is only accountable to themselves.
- Potential learner's misconceptions include:
    - The learner thinks the class is a beginning computer user course.
    - Everyone that contacts a person on the internet is honest.
    - It's okay to reuse a password as long as it's more complex.
    - The sender's email address is always legitimate.
    - Malware only damages Windows computers.
    - Only people on social media are targets.

Instructional Context

- The training is web-based, on-demand, and the learner may take the training whenever they choose.

- The physical learning environment is wherever the learner chooses to take the CBT. They decide where best to do the training.
- Additional accommodations will be provided in the form of text transcripts and audio files.

Technology Inventory

- The learner must have access to a computer or tablet with a modern browser and internet access to complete the CBT.

Transfer Context

- The instruction will be transferable and based on concepts rather than specific application-based techniques to ensure that the material stays relevant and is something the learner can take away and apply to other situations.
- The learner will find value in the provided training as it will make them less vulnerable as they use the internet in everyday tasks such as email, social media, and E-commerce. They will also use what they learned to build experience and confidence as time goes on.
- Support will be available in the form of links to additional cyber safety information as well as referring the learner to Virtue Systems for consultation on more specific problems.

Instructional Impact Based Upon Learner Characteristics

Application of Learning Theories

While age is not an indicator of whether or not one has cyber safety savvy, the target audience as senior citizens and adult learners will respond better to training built with adult learning theories in mind. This CBT will not feature in-classroom learning, but it will still be structured in a way that caters to adult learners. The CBT will clearly outline the learning objectives at the beginning of the lesson, and each module will be uniformly structured. This will not only show the expected outcome, but it will help the learner determine if this course will be useful to them.

People who access the training demonstrate they already have the motivation to learn, but a relevant motivator and examples will be used to make knowledge transfer more likely. It is imperative that the tone used throughout the lessons is clear and free of jargon without being condescending. At no point should the learner feel they are being talked down to because of their age or level of cyber knowledge.

Application of Motivational Theories

The motivational theory employed will be the Expectancy – Value – Cost Model in which the learner feels able to successfully do the task, finds value in it, and any cost of time and resources is justified. Expectancy will come in the form of clear expectations coupled with an appropriate level of perceived task difficulty. The cost impact of this training is minimal, only effort and time are needed and they are justified by the value. The strongest motivational factor for this CBT is value, relevance, context and rationale, and intrinsic benefits will drive seniors to complete this training (Yarborough & Fedesco, 2020).

IMPACT OF A DIVERSE AUDIENCE ON INSTRUCTION

There is a chance of a language barrier due to the organization being based in Arizona, which has a sizeable Hispanic population. Virtue Systems, being a company of just two people, does not have the resources to translate training for other languages, but there are still methods of acquiring cyber safety knowledge. Providing links to translation sites can help determined learners understand the CBT. Additionally, deliberate illustrations and animations will help communicate context, even with a language barrier.

Cultural differences should be minimal when it comes to cyber safety. Nobody wants to be a victim of a scam, or have their password stolen, regardless of their background. This training is aimed toward making safe internet choices; safety practices should not discriminate.

Goal and Task Analysis – Module 5

GOAL ANALYSIS

INSTRUCTIONAL GOAL

Recognize scams and fraudulent activity in web pages, emails, and texts. Demonstrate password management skills by creating a complex password and enabling two-factor authentication. Employ safe privacy practices on social media and public computers. Protect your devices from online threats by using security software suites, enabling passwords, downloading safely, and reacting appropriately to malware.

TASK ANALYSIS METHOD

Topical Analysis

I went through a few iterations of identifying my task analysis method before I settled on Topical. Initially I wanted to make it a hybrid of Topical and Procedural because while some concepts and principles were firmly in the cognitive domain, there was also places where procedures seemed logical.

Since we were limited to one method, I decided to try and make everything procedural, but the some of the concepts were square pegs trying to be fit into round holes and I couldn't get my thoughts across as clearly as I'd like.

I ended up going strictly to topical because, while there are a few places for procedures to fit nicely, it makes more sense to treat everything as a concept and add illustrative training aids where applicable while not restricting concepts to specific procedures because technology is so fluid.

TASK ANALYSIS

1. **Recognize scams and fraudulent activity in web pages, emails, and texts.** (Principle)
    - Identify unsafe or masked links (Concept)
        - Links
        - URLs
        - Email addresses
    - Identify a Scam (Concept)
        - Unsolicited requests for money
        - "Too good to be true."
    - Identify Fraudulent Content (Concept)
        - Phishing – Attempts to steal information such as login credentials

2. **Demonstrate password management skills by creating a complex password and enabling two-factor authentication.** (Principle)
    - Complex passwords (Concept)
        - Methods to create passwords
    - Unique Passwords (Concept)
        - Password management software
    - Two-Factor Authentication (Concept)
3. **Employ safe privacy practices on social media and public computers.** (Principle)
    - Social Media (Concept)
        - Privacy Settings
        - Safe posting practices
    - Public Computers (Concept)
        - Browsers
            - Cookies & History
            - Logins
        - Downloads
        - Secure Network
4. **Protect your devices from online threats by using security software suites, enabling passwords for devices, downloading safely, and reacting appropriately to malware.** (Principle)
    - Tools that protect your computer (Concept)
        - Security Suites
            - Antivirus/malware detection
            - Firewall software
            - Password Management
    - Enabling Passwords and Passcodes (Concept)
        - Computer
        - Phone
        - Wifi network router
        - Devices

- Safe Downloads (Concept)
- What to do when your computer is infected (Concept)
    - Ransomware
    - Virus/Malware

Instructional Objectives – Module 5

TERMINAL OBJECTIVES AND ENABLING OBJECTIVES

- [Terminal Objective 1] - Given examples of web pages, emails and texts, learner will be able to recognize scams and fraudulent activity 90% of the time. *Terminal Objective 1 and all Enabling objectives are at Understanding level in the Cognitive Domain*
    - [Enabling Objective 1a] Given examples of web pages and emails, identify unsafe or masked links, URLs, and email addresses 90% of the time.
    - [Enabling Objective 1b] Given examples of web pages, texts, and emails, identify a scam in a message or webpage 90% of the time.
    - [Enabling Objective 1c] Given examples of web pages, texts, and emails, identify a fraudulent message or webpage 90% of the time.

- [Terminal Objective 2] - Given National Institute of Standards and Technology's (NIST) recommended password criteria, construct a complex password and enabling two-factor authentication. *Applying Level in the Cognitive Domain*
    - [Enabling Objective 2a] Given NIST criteria, construct complex passwords. *(Applying in Cognitive domain)*
    - [Enabling Objective 2b] Given examples of login screens, demonstrate successful two-factor authentication. *(Applying in Cognitive domain)*

- [Terminal Objective 3] – Given examples of privacy settings**,** apply safe privacy practices on social media and public computers 90% of the time. (*Applying Level in Cognitive domain*)
- [Terminal Objective 4] - Given examples of internet threats, learner will be able to identify the appropriate preventative or reactive countermeasure 90% of the time *(Understanding Level in Cognitive domain)*

Enabling Objectives Matrix & Supporting Content – Module 6

Title of the unit/module:

Passwords and Authentication

Brief description of target audience:

Senior Citizens that are not comfortable using modern cyber and internet technology.

List Terminal Objective Here:

Given National Institute of Standards and Technology's (NIST) recommended **password criteria, construct a complex password and enable two-factor authentication.**

List Pre-Instructional Strategy:

Behavioral Objectives

Enabling Objective	Level on Bloom's Taxonomy	Learner Activity (What would learners do to master this objective?)	Delivery Method (Group presentation/lecture, self-paced, or small group)
Given NIST criteria, construct complex passwords.	Applying	Learner will be given a complex password cheat sheet and webpage mockup (javascript) for creating a password. This will be the equivalent of an evaluation with the option to try again for practice.	Self-paced
Given examples of login screens, demonstrate successful two-factor authentication.	Applying	While I would love to use an actual phone it will just be a sequenced graphic simulation do to time and programming constraints. I intend to show the learner 2 examples of a login that requires 2-factor authentication, one for a smart phone text, one for an email text. They will use the dummy login page and graphic depictions of a phone and webmail to authenticate, successful logins on both will be passing the evaluation.	Self-paced

This is a printable of the *Password Tips & Tips Quick Reference Guide* I made for Enabling Objective 1 which will help users construct complex passwords.

VIRTUE SYSTEMS
Technology. Simplified.

Password Tips & Tricks

Do - Follow password requirements per website
Do - Use at least 8 characters
Do - Use at least 1 number and 1 symbol
Do - Use a mixture of capital and lowercase letters

Don't - Use the same password for multiple sites
Don't - Use strings of letters that form words
Don't - Use keyboard patterns like "asdfghjk"
Don't - Use names or personally idendifiable information
And most importantly:
Don't use the word PASSWORD

Generate a Password Using the Phrase Method

Make up an easy to recall phrase based on an actual event. Use the first letter of each word to form a password, use capital letter, numbers and symbols when they make sense.

"I ate cheesecurds at the state fair in 02"
becomes:
I8c@tsfi02

References

National Institute of Standards and Technology. (2017). NIST special publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management (800-63B). https://pages.nist.gov/800-63-3/sp800-63b.html

Yarborough, C., & Fedesco, H. (2020, March 27). *Motivating students*. Center for Teaching. Retrieved June 11, 2021, from https://cft.vanderbilt.edu/guides-sub-pages/motivating-students/