Design Document for Cyber Safety CBT

By [**Anne Carlsen**]

Portfolio: https://annec.net/767.html

Purpose of the Course	Provide free of charge cyber safety computer-based training (CBT) module for senior citizens accessing virtuesystems.net to promote the company while limiting unnecessary pro bono services.
Audience Description	Senior Citizens with basic computer skills, access to a computer and internet, and who want to improve their cyber skills and knowledge.
Major Course Objectives (Terminal)	• **Terminal Objective 1** o Given examples of web pages, emails and texts, learner will be able to recognize scams and fraudulent activity. • **Terminal Objective 2** o Given recommended password criteria, learner will be able to construct a complex password and enable two-factor authentication. • **Terminal Objective 3** – (Not featured in ID project) o Given examples of privacy settings**,** apply safe privacy practices on social media and public computers. • **Terminal Objective 4** – (Not featured in ID project) o Given examples of internet threats, learner will be able to identify the appropriate preventative or reactive countermeasure.

Course Enabling Objectives	TO 1 • Enabling Objectives o Given examples links, URLs and email addresses, identify unsafe or masked links, URLs, and email addresses with 80% accuracy. o Given unsafe or masked links, identify a scam or fraudulent activity in a message or webpage with 80% accuracy. TO 2 • Enabling Objectives o Given password criteria, construct Complex Passwords. o Given examples of login screens, execute successful two-factor authentication.
RLO Enabling Objective	Instead of a single enabling objective for the RLO, I am using the whole Terminal Objective 2 because the second enabling objective is tied closely to the first and it makes more sense than to leave it to its own RLO since it’s only one slide and a question. TO2: • EO 1: Given password criteria, construct Complex Passwords. • EO 2: Given examples of login screens, execute successful two-factor authentication.

Learning Assessment for Course	There will not be a formal assessment, but there will be an ungraded Knowledge Check at the end of each terminal objective module. Assessments are ungraded to promote learning rather than add stress with a message of pass/fail. For the TO 1 Knowledge Check, the learner is provided examples of masked/unsafe links and email addresses, fraudulent URLs and possible scam messages and asked to identify them. For the TO 2 Knowledge Check, the learner is given a series of multiple choice and true/false questions followed by two simulation questions, one simulating password creation and one simulating two-factor authentication.

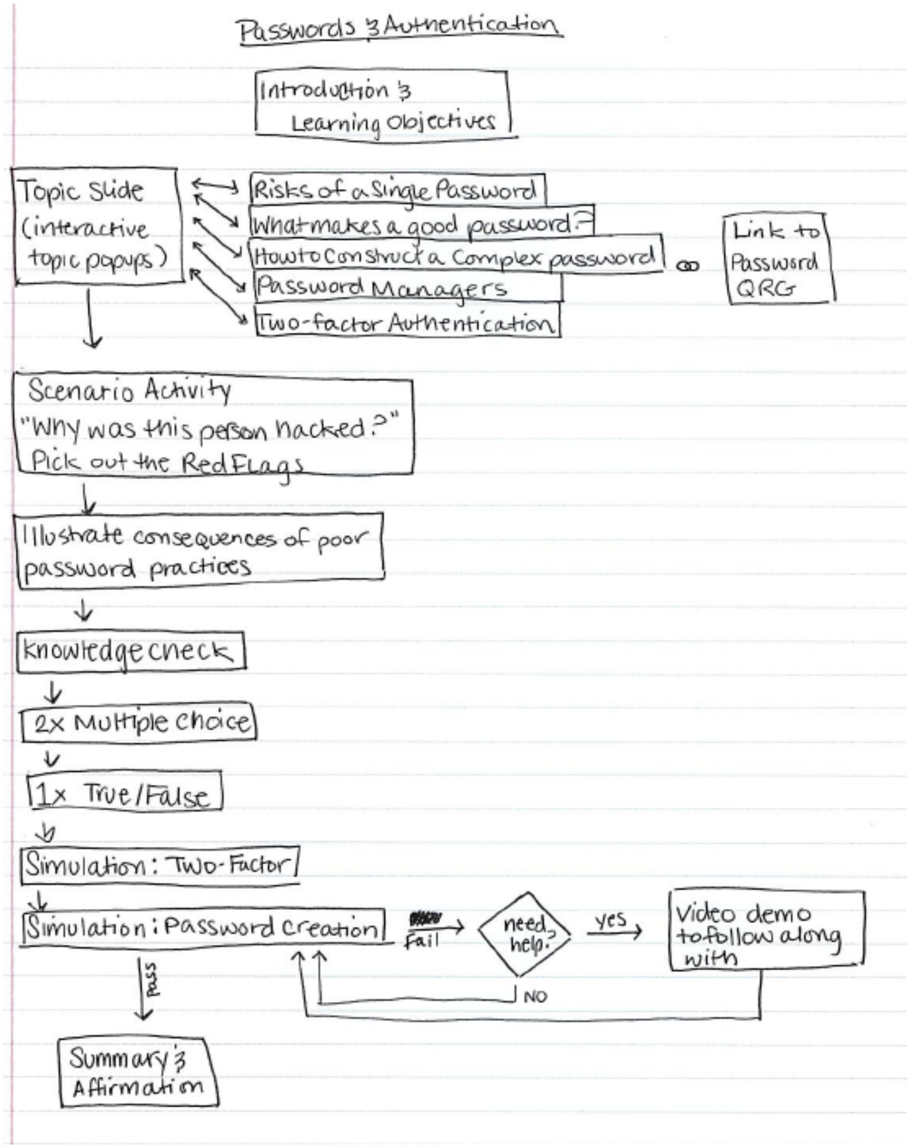
Learning Assessment for RLO

Sample Questions :

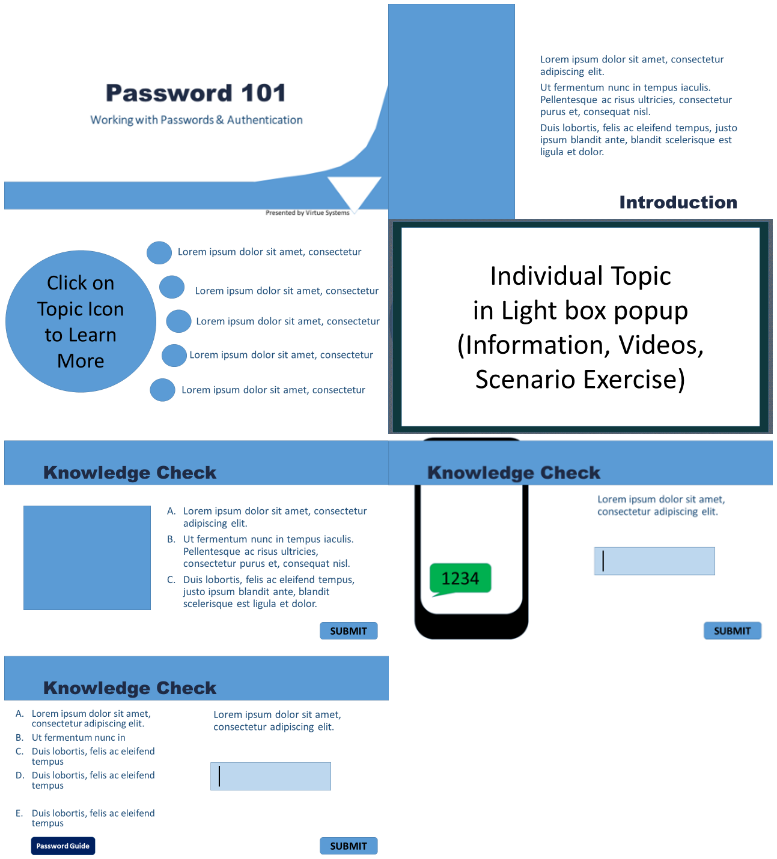
- Using your password quick reference guide, determine which answer is the strongest password.
  - PASSWORD123 Incorrect – Any password containing the word password is not secure.
  - admin2021! Incorrect – While it’s tempting to use the default password given to you from a technology manufacturer, it also makes it very easy to guess.
  - 2wL@pw&m Correct! – This password is at least 8 characters, and has a combination of uppercase/lowercase letters, numbers and symbols.
  - July151945 Incorrect – This password has a specific date, possibly a birthdate. This is the type of additional information you don’t want hackers to have!
- True or False: Passwords should be written down and placed where you can find them easily.
  - True Incorrect – Writing down passwords is not recommended, but if you need to write down passwords, store them securely!
  - False Correct! – Hand-written passwords placed where you can find them are also where other people may find them. Secure handwritten passwords or use a password manager.
- Two-factor authentication simulation
- Password creation simulation (branching scenario allows learner to view a previously hidden video demonstration to mimic if first try does not meet password criteria)

Instructional Delivery method for Course (overall)	This instruction will be delivered as self-paced computer-based training available on the company website.
Instructional Strategy for RLO	• Tutorial o Presentation o Guidance (supplemented with Quick Reference Guide) o Practice (Knowledge Check T/F and Multiple Choice to reinforce concepts) o Assessment (Knowledge Check Simulation Questions)
Media	This CBT will use Articulate Storyline and video demos in will be created in Camtasia.
508 Accommodations	Fonts 18pt+, High Contrast Colors, Audio narration and CC of slides, Alt text
Course Structure Description	Modules can be taken in order or individually. • Module 1: Identify Scams and Fraudulent Activity • **Module 2: Passwords and Authentication** • Module 3: Internet Privacy Best Practices • Module 4: Computer and Internet Security Best Practices
Seat Time of Course	1-2 hours depending on user pace.
Seat Time of RLO	15-20 minutes depending on user pace.

RLO Outline	Passwords and Authentication 1. Introduction and Storyline Player Demo 2. Risks of a Single Password 3. What makes a good password? 4. How to construct a complex password a. Password Tips & Tricks Quick Reference Guide 5. Password Managers 6. Two-Factor Authentication 7. Scenario – “Why was this guy hacked?” Pick out the Red Flags 8. Knowledge Check a. Questions b. Simulations i. Password Creation Branching Scenario with video demo 9. Summary

RLO Flowchart	 Passwords & Authentication Introduction & Learning Objectives Topic Slide (interactive topic popups) Risks of a Single Password What makes a good password? How to Construct a Complex password Password Managers Two-factor Authentication Link to Password QRG Scenario Activity "Why was this person hacked?" Pick out the Red Flags Illustrate consequences of poor password practices knowledge check 2x Multiple choice 1x True/False Simulation: Two-Factor Simulation: Password creation Fail need help? yes Video demo to follow along with NO PASS Summary & Affirmation
Screens/Pages in RLO	11 primary Screens +7 Light box popups

Knowledge Checks or Other Assessments or Practices for RLO	__2__Dichotomous (T/F, Y/N, etc.) __1__Multiple Choice __0__Multiple Select (Select all the Red Flags exercise) __0__Drag and Drop __2__Custom – o 1) Create Password simulation (Instructions with password requirements, text form for password submission, will use JavaScript) o 2) Use Two-factor Authentication simulation (Image of a smartphone with a text message of a number, learner enters number into text form to authenticate) __0__Other – describe
Rollovers/click events	__13_Rollovers __22__Click Events (including 5 quiz interactions)
RLO Navigation	I'll be using Storyline's modern navigation with text descriptions enabled, I will ensure the usability features are enabled. Upon opening the CBT, the learner will have the option to play a quick demo video showing how to use the navigation. All interactive features (buttons/icons) are high contrast and easy to tell if the user is hovering over it.

Screen Layouts for RLO	 Password 101 Working with Passwords & Authentication Presented by Virtue Systems Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut fermentum nunc in tempus iaculis. Pellentesque ac risus ultricies, consectetur purus et, consequat nisl. Duis lobortis, felis ac eleifend tempus, justo ipsum blandit ante, blandit scelerisque est ligula et dolor. Introduction Click on Topic Icon to Learn More Lorem ipsum dolor sit amet, consectetur Lorem ipsum dolor sit amet, consectetur Lorem ipsum dolor sit amet, consectetur Lorem ipsum dolor sit amet, consectetur Lorem ipsum dolor sit amet, consectetur Individual Topic in Light box popup (Information, Videos, Scenario Exercise) Knowledge Check A. Lorem ipsum dolor sit amet, consectetur adipiscing elit. B. Ut fermentum nunc in tempus iaculis. Pellentesque ac risus ultricies, consectetur purus et, consequat nisl. C. Duis lobortis, felis ac eleifend tempus, justo ipsum blandit ante, blandit scelerisque est ligula et dolor. SUBMIT Knowledge Check 1234 Lorem ipsum dolor sit amet, consectetur adipiscing elit. SUBMIT Knowledge Check A. Lorem ipsum dolor sit amet, consectetur adipiscing elit. B. Ut fermentum nunc in C. Duis lobortis, felis ac eleifend tempus D. Duis lobortis, felis ac eleifend tempus E. Duis lobortis, felis ac eleifend tempus Lorem ipsum dolor sit amet, consectetur adipiscing elit. Password Guide SUBMIT
Development Tools for RLO	Primary authoring tool: Articulate Storyline 360 Video tool: Techsmith Camtasia 2021 storyboarding tool: Microsoft PowerPoint
Ownership	Anne Carlsen will develop the initial course; however, Virtue Systems will maintain the course.
Development Time of RLO	2 weeks

Support requirements for RLO and course	Level of support: Low - No additional support needed.
Project Sign-off [optional]	Please sign below indicating agreement with the proposed course plan and approving start-up of the storyboard and development phases.
	Instructional Designer Date
	Project Manager/Sponsor Date