

Title Slide: 1.0 A Second Chance: Exploring Two-Factor Authentication	
OST	Files / Images
Heading - A Second Chance: Exploring Two-Factor Authentication	Fair Use
Audio/VO	Animation / Visual
Welcome to two factor authentication, concepts and applications. Select 'Next' to get started.	When slide displays, fade in the heading, and then subheading. Image will be a stock image of some type of 2FA method (USB key, circle-lock, badge to scan etc)
Programming Notes: Remove the navigation button for "previous". For all slides, Include the title slide text on screen, unless the title slide is in <i>italics</i> within the storyboard.	

Slide Name: 2.0 Mastering 2FA: What You'll Learn	
OST	Files / Images
The learner will: - Identify which 2FA types are present in their daily life. - Compare 2FA methods for the everyday user, to those in a corporate setting. - Differentiate between the 2FA methods for data security and physical security.	Fair Use
Audio/VO	Animation / Visual
The learner will identify which 2FA types are present in their daily life. Compare 2FA methods for the everyday user, to those in a corporate setting. The learner will be able to differentiate between the 2FA methods for data security and physical security.	Animate each bullet point as VO starts. Use a simple fade-in for text.

Programming Notes: Have each line item slide in from the left. Space the timing for Animation / Visuals at a pace for the voiceover to speak to each one.

Slide Name: 3.0 2FA in Everyday Life

OST	Files / Images
There's no doubt you're familiar with using your email to create a new account online. After signing up, an account may: • Require a separate code from email to be confirmed. • Give the option to login with facial recognition or a phone fingerprint scanner. • Require a separate code generation app to login. These are all common examples of 2FA. [Summary Sentence] Two factor authentication will ensure you have an extra layer of protection for your sensitive data. It's not foolproof, but it will significantly strengthen your security presence online. It's recommended to enable it wherever possible.	Fair Use
Audio/VO	Animation / Visual
There's no doubt you're familiar with using your email to create a new account online. Let's review some examples of 2FA after creating an account. Select each [design item] to reveal each option.	Fade in the introductory sentence near the top of the slide.
Programming Notes: Fade in the introductory sentence near the top of the slide. Use a [design item] to have the user select a (tab, shape etc.) to reveal each bullet point. The [Summary Sentence] will be triggered once all design items have been viewed after a delayed time has passed. The [Summary Sentence] should be the focal point of the screen, or the only OST visible when triggered.	

Slide Name: 4.0 Doubling Down: What makes 2FA essential?

OST	Files / Images
(Title) Doubling Down: What makes 2FA essential? • Hackers are constantly searching for more creative ways to steal account data and passwords. • You may think a complicated password with special characters is enough protection.	Fair Use

• Even a castle will have multiple layers of protection. • Why not add those same layers of protection for your online bank accounts, social media, or even the physical devices that are most important to you?	
Audio/VO	Animation / Visual
On this slide, let's compare 2FA to how a castle has multiple layers of protection for its defense against attackers.	On each reveal of new content, have each castle image slide in from the bottom of the screen. Ease-in the Animation / Visual to a stopping point. Use the introduction video as a reference.
Programming Notes: Using the castle assets, start with the castle on the forest background. Have a pop-up window centered above the castle to include the content in order. For bullet one and two, have the scene background remain the same but display content with a 'continue' button. For the 3rd bullet, have the water enter the scene. For the 4th bullet, have the door enter the scene. — View Example	

Slide Name: 5.0 How Corporations are Ditching the Single-Layer	
OST	Files / Images
Corporations also use 2FA to keep your data safe. Places such as data centers, or corporate offices, have an obligation to keep data that can be physically accessed safe and secure. Let's get familiar with some corporate 2FA solutions: • Hardware verification (USB Keys) ◦ Employers may provide their staff with a USB key for 2FA. ◦ The USB key will be required when prompted by their workstation, to log-in, or access certain software. ◦ The user will plug the USB key in, and typically press a capacitive section of the key, or press a confirm button on screen. • VPN Connection ◦ Also known as a virtual private network, a corporation may limit access to the public internet for an employee. ◦ Requiring a VPN will help protect data privacy, by encrypting network traffic between the user and the internet. ◦ The VPN will also allow corporations to provide controlled access between the user and the internet. ◦ VPNs are great tools for software related 2FA, as long as the VPN itself requires multiple factors of authentication (corporate network connection, password required) • Pin Code Device	Fair Use

○ It's common practice for a corporation to require employees to use a badge as a form of identification, and a way to access doors on campus. ○ Certain doors that require a badge scan may also require the user input a PIN number as a second form of authentication. ● Biological 2FA (Eyescan, Fingerprint) ○ Similar to a PIN code to access sensitive areas, a form of eye scanner, or fingerprint scanner may be required to access sensitive areas as well.	
Audio/VO	Animation / Visual
Let's explore how corporations are ditching the single-layer. [Pause Continue] Corporations are also responsible for keeping your data safe. Places such as data centers, or corporate offices, have an obligation to keep data that can be physically accessed, safe and secure.	Fade text in when voiced.
Programming Notes: This slide will have a tabbed interaction with hover, selected, and visited states for each tab button. Introductory voiceover text will be displayed above the tabbed sections, while the tab module itself remains grayed out. Once the voiceover intro has completed, the module can become fully colored, indicating interaction. "Let's get familiar..." will prompt when to make this module available. Use Bullets for tabbed module data.	

Slide Name: [Scenario] 6.0 Choosing the Best Two Layers	
OST	Files / Images
[Scene 1] Hey, thank you for coming as soon as you could. I'm Matthew, the director of security for Consistent Health. [Scene 2] Another health insurance company was recently breached and hackers locked 70% of their computers. We brought you in to consult us on two-factor authentication. [Scene 3] We want to implement new security policies for the entire company, to enhance our security to avoid the same fate. [Scene 4] Before we get started, I'll be here to help provide assistance, should you require any additional context. Just select my icon in the top-right. [Help Icon] See, I'll be with you along the way. Don't hesitate to reach out if you need clarification.	Fair Use
Audio/VO	Animation / Visual

[Scene 1] Hey, thank you for coming as soon as you could. I'm Matthew, the director of security for Consistent Health. [Scene 2] Another health insurance company was recently breached and hackers locked 70% of their infrastructure. We brought you in to consult us on two-factor authentication. [Scene 3] We want to implement new security policies for the entire company, to enhance our security and avoid the same fate. [Scene 4] Before we get started, I'll be here to help provide assistance, should you require any additional context. Just select my icon in the top-right. [Scene 5] Let's get started with our first security improvement.	Use in-app assets for Matthew's avatar, and speech bubbles to create the scene. Between each scene, fade-in the speech bubble text and choose appropriate avatar emotions with each line. Background image can be an office setting or security room. On scene 4, highlight the icon near the avatar, and before continuing to scene 5, animate the icon to slide to the top-right of the slide.
Programming Notes: OST and VO are separated by scenes. Each scene is separated with an interaction from the user (Continue button for example). When the learner selects a choice that can branch based on the answer, that will be labeled as a different slide.	

Slide Name: [Scenario] 6.1 Choosing the Best Two Layers			
OST		Files / Images	
[Scene 1] First, let's start at the entrance of our corporate office. The physical security to the building, and safety of our employees is important to us. [Scene 2] What do you think will be the best solution to implement two-factor authentication to the entrance? [Choices] 1. Email 2FA - Require employees to respond to an email after scanning their badge. 2. PIN Code - Change the badge reader to include a number pad that requires a PIN after scanning. 3. VPN - Require employees to connect to the secured network on their device before scanning their badge. [Help Icon] In this case, we will need to consider the best way to upgrade a <u>physical</u> entry with two factors of authentication.²		Fair Use	
Audio/VO		Animation / Visual	
[Scene 1] First, let's start at the entrance of our corporate office. Physical security to the building, and safety of our employees is important to us. [Scene 2] What do you think will be the best solution to implement two-factor authentication to the entrance?		Each answer will be an image that once clicked on, will show a text bubble below with a title. Use fade animations. The state for a selected image can be a simple outline or drop-shadow.	

Programming Notes: PIN Code = Correct Answer. Move on to slide 6.1a after the learner chooses this option. For incorrect answer choice move on to slide 6.1b.

Slide Name: [Scenario] 6.1a Choosing the Best Two Layers (*Correct Answer*)

OST	Files / Images
[Scene 1] I agree, adding a number pad to the badge readers will be a quick and effective way to add 2FA to the main entrance. [Scene 2] The entrance is a physical access point. Scanning the badge is one factor for security, and having each user set a unique PIN number will increase the entrance to two layers of security. [Scene 3] When you're ready, let's move on to our next 2FA solution. [Help Icon] Good job, while email and VPNs are examples of 2FA, for a physical solution, the PIN number is the best answer here.	Fair Use
Audio/VO	Animation / Visual
[Scene 1] I agree, adding a number pad to the badge readers will be a quick and effective way to add 2FA to the main entrance. [Scene 2] The entrance is a physical access point. Scanning the badge is one factor for security, and having each user set a unique PIN number will increase the entrance to two layers of security. [Scene 3] When you're ready, let's move on to our next 2FA solution.	Reflect positive emotion from the avatar, since the learner picked the correct answer.
Programming Notes: Utilize the continue button to move on from each scene. VO will only activate when displayed in the speech bubble. After last VO and OST, jump to slide 6.2	

Slide Name: [Scenario] 6.1b Choosing the Best Two Layers (*Incorrect Answer*)

OST	Files / Images
[Scene 1] Let's think about this, with VPN or Email authentication, these methods are more in line to protect non-physical data. [Scene 2] The entrance to our corporate office is considered a physical access point. Which option do you believe will fit best? [Help Icon] In this scenario, Email or VPN authentication will require an employee to check their work device. A PIN number seems to be the most accessible option here.	Fair Use

Audio/VO	Animation / Visual
[Scene 1] Let's think about this, with VPN or Email authentication, these methods make more sense to protect non-physical data. [Scene 2] The entrance to our corporate office is considered a physical access point. Which option do you believe will fit best?	Reflect the avatar in a thinking pose, to invoke the consideration for a different answer.
Programming Notes: After continuing from [Scene 2], the slide will navigate back to 6.1 to have the learner attempt another answer. VO will only activate when displayed in the speech bubble.	

Slide Name: [Scenario] 6.2 <i>Choosing the Best Two Layers</i>	
OST	Files / Images
[Scene 1] Now we're inside at the tech stop desk. This is where employees pick up their work devices like laptops or tablets. [Scene 2] Let's consider the next 2FA upgrade for this station. What solution would make the most sense for implementing 2FA for work devices? [Choices] 1. Circle Lock - A personnel control device that allows one person at a time to pass to a secure area. 2. Handprint - Requires the user to scan their handprint in order to login to the work device. 3. USB Key - An easy to carry USB device that can plug into a work device to provide authentication. [Help Icon] Think about the capabilities of the typical laptop or work tablet. Which 2FA would make the most sense to implement for a user to login?	Fair Use
Audio/VO	Animation / Visual
[Scene 1] Now we're inside at the tech stop desk. This is where employees pick up their work devices like laptops or tablets. [Scene 2] Let's consider the next 2FA upgrade for this station. What solution would make the most sense for implementing 2FA for work devices?	Reflect the avatar bringing focus to the tech stop desk. Afterwards have the avatar reflect a thinking pose when asking the question for [Scene 2]. Each answer will be an image that once clicked on, will show a text bubble below with a title. Use fade animations.
Programming Notes: Correct answer is 3 – USB Key. Have the slide jump to 6.2a for the correct answer. The other incorrect answers will jump to slide 6.2b. Voice over will only activate when VO text is visible.	

Slide Name: [Scenario] 6.2a Choosing the Best Two Layers (<i>Correct Answer</i>)	
OST	Files / Images
[Scene 1] Great choice! A USB key is a physical device the user can keep secure on their person. [Scene 2] The key can be used in combination with their password to log into the work device. Let's move on.	Fair Use
Audio/VO	Animation / Visual
[Scene 1] Great choice! A USB key is a physical device the user can keep secure on their person. [Scene 2] The key can be used in combination with their password to log into the work device. Let's move on.	Reflect the avatar in a positive pose for the correct answer.
Programming Notes: VO will only activate when displayed in the speech bubble. Continue button will jump to scenario 6.3	

Slide Name: [Scenario] 6.2b Choosing the Best Two Layers (<i>Incorrect Answer</i>)	
OST	Files / Images
[Scene 1] There may be a better choice, try to think about the capability of a tablet or laptop. [Scene 2] We want to pick the 2FA method that works best for a portable device.	Fair Use
Audio/VO	Animation / Visual
[Scene 1] There may be a better choice, try to think about the capability of a tablet or laptop. [Scene 2] We want to pick the 2FA method that works best for a portable device.	Reflect the avatar in a thinking pose since the answer choice was incorrect.
Programming Notes: When continue is selected, the slide will jump to 6.2 to have the learner restart this scenario. VO will only activate when displayed in the speech bubble.	

Slide Name: [Scenario] 6.3 Choosing the Best Two Layers	
OST	Files / Images
[Scene 1] We're now at the desk of one of our Data Specialist team members. I think we've done enough 2FA on the physical side for now. [Scene 2] Could you help me find the best 2FA option for our Database Management Software? This is a very sensitive program, and is only ever accessed on site through our work network. [Scene 3] Which solution do you think is best? 1. VPN (Virtual Private Network) - Requiring a user to connect to the VPN can be a way to verify the user has access to a proper network before logging in. 2. Fingerprint Scanner - This will require a user to scan their fingerprint before logging into the Database Management software. 3. Text to Personal Phone - This will have a uniquely generated six-digit number sent to the user. Afterwards the user enters this to sign-in to the software. [Help Icon] For this scenario, first think about how software can be secured. In addition, consider that personal devices are not as secured as work assigned devices.	Fair Use
Audio/VO	Animation / Visual
[Scene 1] We're now at the desk of one of our Data Specialist team members. I think we've done enough 2FA on the physical side for now. [Scene 2] Could you help me find the best 2FA option for our Database Management Software? This is a very sensitive program, and 2FA will enhance its security. [Scene 3] Which solution do you think is best?	[Scene 1] Avatar reflects a neutral pose while in front of a computer screen. [Scene 2] Avatar brings attention to the screen. [Scene 3] Avatar reflects a thinking pose.
Programming Notes: Upon the selection of option 1 VPN (correct) the slide will jump to 6.3a. All other selections (incorrect) will jump to 6.3b. VO will only activate when displayed in the speech bubble.	

Slide Name: [Scenario] 6.3a Choosing the Best Two Layers (<i>Correct Answer</i>)	
OST	Files / Images
[Scene 1] I'd have to agree. We program the VPN to connect after the user enters their device password. [Scene 2] The VPN itself also requires the user to connect to the company's secured network. This essentially provides multiple layers of security for the software. [Help Icon] Great job, keep in mind not all VPNs are considered 2FA. In this case, the requirement of a password and a specific network connection qualify this VPN as two-factor authentication.	Fair Use

Audio/VO	Animation / Visual
[Scene 1] I'd have to agree. We program the VPN to connect after the user enters their device password. [Scene 2] The VPN itself also requires the user to connect to the company's secured network. This essentially provides multiple layers of security for the software.	The avatar will reflect a positive pose due to the correct answer being selected.
Programming Notes: VO will only activate when displayed in the speech bubble. This slide will jump to 7.0 after selecting the continue button.	

Slide Name: [Scenario] 6.3b Choosing the Best Two Layers (<i>Incorrect Answer</i>)	
OST	Files / Images
[Scene 1] Let's reconsider this option. A fingerprint scanner would be expensive to add to all computers, since the option is not built in. [Scene 2] Requiring a 2FA code from a phone is a good idea, but in this context let's avoid using an employee's personal phone. [Help Icon] The VPN (Virtual Private Network) is another great choice for securing software. In this case the VPN would be the better choice over requiring a user to incorporate their personal device.	Fair Use
Audio/VO	Animation / Visual
[Scene 1] Let's reconsider this option. A fingerprint scanner would be expensive to add to all computers, since the option is not built in. [Scene 2] Requiring a 2FA code from a phone is a good idea, but in this context let's avoid using an employee's personal phone.	Reflect the avatar in a thinking pose.
Programming Notes: [Scene 1] Let's reconsider this option. A fingerprint scanner would be expensive to add to all computers, since the option is not built in. [Scene 2] Requiring a 2FA code from a phone is a good idea, but in this context let's avoid using an employee's personal phone. Slide will return to 6.0	

Slide Name: 7.0 Remaining Compliant with "Two Layers"	
OST	Files / Images

To most, two-factor authentication can seem like an inconvenience, especially when it becomes a requirement. In your personal life, a mobile banking app may require 2FA for example. This is more commonplace as hackers continue to find ways around simple security measures, such as a complex password. Compliance requirements can vary depending on the sensitivity of the data you access. The type of 2FA you experience at work and at home can vary, but both serve to provide additional security.	Fair Use
Audio/VO	Animation / Visual
To most, two-factor authentication can seem like an inconvenience, especially when it becomes a requirement.	
Programming Notes: Fade-in text one paragraph at a time.	

Slide Name: Slide 8.0 Recognizing Authentication Categories	
OST	Files / Images
[Scene 1] It's determined by now that a minimum of two forms of authentication are required to provide enhanced security for valuable data, or an access point. [Scene 2] Let's take a moment to recognize how some authentication factors are categorized. • Hardware can be associated with devices that are physical components of a device or system. Some examples include: ◦ USB keys ◦ Smart Cards ◦ Badges • Software authentications are more commonplace and budget friendly. These are associated with intangible applications. ◦ Email or Text Message authentication ◦ A code generator software or app ◦ A VPN network • A biological based method of authentication would rely on the unique aspects of a user's body for verification. ◦ Fingerprint sensor ◦ Facial Recognition	Fair Use

○ Eyescanner / Iris Recognition It's important to recognize the diverse category of authentication methods as hackers continue to use creative ways to bypass 2FA.	
Audio/VO	Animation / Visual
[Scene 1] It's determined by now that a minimum of two forms of authentication are required to provide enhanced security for valuable data, or an access point. [Scene 2] Let's take a moment to recognize how some authentication factors are categorized.	
Programming Notes: VO will activate as text fades in. Use icons for hardware, software, and biological 2FA methods respectively, revealing the related bullet point information.	

Slide Name: 9.0 Become Less of a Target	
OST	Files / Images
Become familiar with some tactics hackers use to access your data: • Social Engineering: A hacker may pose as a trusted source like a relative, a celebrity, or a legitimate organization • Password Forcing: Hackers could use automated tools to guess your password. • Phishing Links: A deceptive link could be clicked on to trick you into typing your password on a fake website with a slightly different URL.	Fair Use
Audio/VO	Animation / Visual
Become familiar with some tactics hackers use to access your data, such as social engineering, password forcing, and phishing links.	
Programming Notes: Have text fade at start for VO. When VO is complete, allow the user to move onto the bullet points. Slide will continue to 9.0	

Slide Name: [Knowledge Check] 10.0 Let's Review What We've Learned	
OST	Files / Images
The following section will review what we've learned so far about 2FA. Feel free to review previous content before we continue.	Fair Use
Audio/VO	Animation / Visual
The following section will review what we've learned so far about 2FA. Feel free to review previous content before we continue.	Text Fade-in
Programming Notes: Fade text in as VO begins reading. Show avatar with a graduation cap in an excited pose.	

Slide Name: [Knowledge Check] 10.1 Let's Review What We've Learned	
OST	Files / Images
How does two-factor authentication play an important role when protecting your online accounts and devices? 1. Strong passwords alone are a great method for using 2FA. 2. 2FA offers an extra layer of security, similar to a castle using multiple methods of defense. (Correct Answer) 3. Hackers are usually not interested in stealing social media accounts. 4. 2FA makes it impossible for hackers to steal your data. Feedback for each answer choice: 1. Although having a strong password is a recommended method of additional security, they are not considered sufficient on their own. 2. Correct, if your password is breached, a second authorization can prevent your account from being accessed. 3. Social media accounts can be valuable for hackers. They may use your account to hack others for example. 4. While 2FA does make it significantly harder, it	Fair Use

doesn't guarantee complete protection from data breaches.	
Audio/VO	Animation / Visual
How does two-factor authentication play an important role when protecting your online accounts and devices?	
Programming Notes: Fade in the question during voiceover, then fade in each answer choice below.	

Slide Name: <i>[Knowledge Check] 10.2 Let's Review What We've Learned</i>	
OST	Files / Images
Which of the following is an example of a biological method of two-factor authentication? - Using a code generator through a mobile phone in combination with a password. - Using a PIN code in combination with a badge scan. - Using a code on a text message in combination with a password. - Using a fingerprint scan in combination with a badge scan. (correct answer) Feedback for each answer choice: - Both methods mentioned are using technology, and don't require a biological method. - Both methods mentioned are using technology, and don't require a biological method. - Both methods mentioned are using technology, and don't require a biological method. - Correct, using a fingerprint as part of the 2FA process is considered a biological factor.	Fair Use
Audio/VO	Animation / Visual
Which of the following is an example of a biological method of two-factor authentication?	

Programming Notes: Fade in the question during voiceover, then fade in each answer choice below.

Slide Name: *[Knowledge Check] 10.3 Let's Review What We've Learned*

OST	Files / Images
Match each authentication method to the category that best matches. • Hardware 2FA ○ A badge Scanner ○ A USB Key • Software 2FA ○ Code via Email ○ Code via Text Message ○ A Code Generator App ○ A VPN network • Biological 2FA ○ Fingerprint Sensor ○ Facial Recognition ○ Iris Scanner	Fair Use
Audio/VO	Animation / Visual
Match each authentication method to the category that best matches.	
Programming Notes: Each bullet will be the category. Create each sub-bullet as an item for matching to the parent-category. Avoid drag-and-drop for accessibility.	

Slide Name: *Show Score from Knowledge Check*

Passing Score	75%
---------------	-----

Slide Name: *[Scenario] 11.0 A Tale of Two Users*

OST	Files / Images
-----	----------------

Which user are you? Explore the following scenario of two people who frequently use social media and browse the internet. Andrew takes his security seriously, after he saw the impact of how identity theft affected a family member. Yenni is less mindful of securing her online data and has been lucky so far with her online connectivity. [Continue Button] Select a character to continue:	Fair Use
Audio/VO	Animation / Visual
Which user are you? Explore the following scenario of two people who frequently use social media and browse the internet. Andrew takes his security seriously, after he saw the impact of how identity theft affected a family member. Yenni is less mindful of securing her online data and has been lucky so far with her presence online. [Continue Button] Select a character to continue:	Andrew is on the left side of the screen. Yenni is on the right side of the screen. Both avatars are showing a wave pose at the user.
Programming Notes: Layout is a split screen of both characters. Their buttons are centered on their half of the screen with the avatar above the button. Buttons will reflect the names “Andrew” and “Yenni” respectively. Selecting Andrew will continue to 11.1a. Selecting Yenni will continue to 11.1b. (Use A and B identifiers for the scenario. A = Andrew and B = Yenni)	

Slide Name: 11.1a A Tale of Two Users	
OST	Files / Images
[Scene 1] Andrew is a business analyst for a large pharmacy company. He works from home but also uses his work computer to access his professional network on LinkedIn. [Scene 2] Let's observe how Andrew logs into his account. Since he takes data seriously, he uses 2FA. [Scene 3] <i>No text (See animation/visual)</i> [Scene 4] Andrew has logged in successfully with no issues!	Fair Use
Audio/VO	Animation / Visual
Let's see how Andrew is with his online account data.	[Scene 3] Show a screen of a mobile 2FA authentication app, next to the login screen of the computer.

Programming Notes: On [Scene 3] require the user to type the authentication that shows in the phone screen. Voiceover plays prior to any animation.

Slide Name: 11.2a A Tale of Two Users

OST	Files / Images
[Scene 1] Well done! Andrew uses some best practices when it comes to securing his account. [Scene 2] Other than 2FA it's a good idea to regularly change passwords, use complex passwords, and avoid suspicious emails. [Scene 3] Now, let's see how this scenario will play out for the other user [Continue Button]	Fair Use
Audio/VO	Animation / Visual
Scene 1] Well done! Andrew uses some best practices when it comes to securing his account. [Scene 2] It's also a good idea to regularly change passwords, use complex passwords, and avoid suspicious emails. [Scene 3] If Andrew didn't use 2FA, it's possible his LinkedIn would've been compromised. [Continue Button] Now, let's see how this scenario will play out for Yenni, our other user. [Continue Button]	The avatar is still on scene but reflects a happy/excited pose.
Programming Notes: This slide will jump to [12.0] If the user has not yet selected the scenario with Yenni, have this slide jump to 11.2b	

Slide Name: 11.2b A Tale of Two Users

OST	Files / Images
[Scene 1] Yenni is a social media influencer, and is sponsored to promote multiple brands. Her income relies on her internet presence, and many people follow her. [Scene 2] Yenni is scrolling a site that asks her to take a test to see which cartoon character fits her personality. Upon clicking the link, it asks for her account details to take the quiz. [Scene 3] Later that day, she receives an email that her account password was changed. Since she doesn't	Fair Use

recognize the request, she checks her account and realizes someone posted on her behalf. They've also been using her account to message her followers to lure them into a phishing scam. [Scene 4] Yenni has learned a valuable lesson in account security. If she had 2FA setup, she likely would have been able to secure her account in time. [Continue Button] Now let's see how this will play out for Andrew, the other user. [Continue Button]	
Audio/VO	Animation / Visual
Let's see how Yenni is with her online data.	[Scene 1] Show Yenni interacting with her phone in some way. [Scene 2] Show a close-up of Yenni on the "quiz" screen, then the screen changing to a sign-in. [Scene 3] Show Yenni checking her phone and being surprised. Show some type of surprised icon as she checks her phone, such as an exclamation mark. Yenni makes a surprised reaction.
Programming Notes: Upon completion of both scenarios, this slide will jump to 12.0. The VO will play prior to the start of any animation in Scene 1. If the user has not yet viewed the scenario with Andrew, jump to 11.1a.	

Slide Name: 12.0 Summarizing 2FA Importance	
OST	Files / Images
We can now recognize the drastic difference in what can happen to users who either take the security of their online data seriously, compared to those who do not. Using two factor authentication can be the difference between losing your account, and even full identity theft. Consequences can be financial, affect your reputation, or even affect those around you once your data is compromised.	Fair Use
Audio/VO	Animation / Visual
We can now recognize the drastic difference in what can happen to users who either take the security of their online data seriously, compared to those who do not. Using two factor authentication can be the difference between losing your account, and even full identity theft. Consequences can be financial, affect your reputation, or even affect those around you once your data is compromised.	

Programming Notes: Animate OST as the voice over begins each line. Animation will be a simple fade-in.

Slide Name:

OST

Files / Images

Audio/VO

Animation / Visual

Programming Notes: