Title:	Tips for Staying Safe Online: Creating and Managing Passwords Video
Introduction:	The Tips for Staying Safe Online Video Series is led through slides as visual markers. Any images in the slides that are important to content, and share any additional information beyond the script, has been included here as Alt text.
Narrator:	Welcome to the Help@Hand Tips for Staying Safe Online; Part 2: Creating and Managing Passwords video. Help@Hand is a California multi-city and county Collaboration created to help shape the future of technology-based mental health solutions and connect people to care across the state. These video tutorials are intended to empower California communities to make informed decisions about how they engage with technology.
Narrator:	This is Course 3 in a 4 course series called Tips for Staying Safe Online Part 2. The videos in this series can be viewed in order or in any order based on your interest. In this video, we'll present strategies for creating and managing online passwords. The following tips can help you create strong passwords that are tough to crack which can reduce the risk of strangers accessing your personal information.
Image:	Display of a sample password with 10 characters. The password is a lowercase f, uppercase P, pound, asterisk, uppercase L, lowercase v, ampersand,2, percent, lowercase a.
Narrator:	The first step is to make your password long. In general, you should aim to include 10 characters. A short password that is only 4-5 characters is much easier to guess than a password that is 10 characters or longer like the one displayed.
Image:	Display of a sample password with 10 characters. The password is a lowercase f, uppercase P, pound, asterisk, uppercase L, lowercase v, ampersand,2, percent, lowercase a. This image moves to highlight the uppercase letters (both P and L) and the lowercase latter's (f,v,a).
Narrator:	When you're creating your password, you should use both uppercase and lower-case letters. As you can see here, not only is the password 10 characters long, but it also contains both upper and lowercase letters.
Image:	Display of a sample password with 10 characters. The password is a lowercase f, uppercase P, pound, asterisk, uppercase L, lowercase v, ampersand,2, percent, lowercase a. This image moves to highlight the numbers 2 and symbols, pound, asterisk, ampersand, percent.
Narrator:	You should also include a variety of numbers and symbols that you can find at the top of your keyboard. Using this password example again, you can see that it contains numbers and symbols that make it harder to guess.
Image:	Displayed on screen are a Social Security Card displaying the card holders full name and social security number, an image depicting "Birthday", and a section of a map meant to depict an "Address".

Narrator: Sometimes, we're tempted to use bits of our personal information within our passwords to make them easier to remember. The problem with this strategy is that scammers may also know some of this information and will use it when trying to guess your passwords. For instance, if a scammer knows your name and address, they may try password combinations that include this information. That's why it's best to keep all personal details out of your passwords.

Image: Display of two different password examples. The first password (on the left) is as follows, uppercase B, less than, plus, question mark, 3, lowercase g, 9, lowercase w, closed bracket, backslash. The second password (on the right) is as follows, uppercase K, lowercase at, lowercase t, lowercase e, 1,2,3.

Narrator: Now that you've learned some tips for creating strong passwords, let's take a moment and review these two different passwords. Which one is more secure? The one on the left or the one on the right?

Narrator: The password on the left would be more difficult for someone to guess because it's long, has upper and lowercase letters, symbols and numbers and does not contain any personal information making it more secure. The password on the right, however, would be very easy to guess because it includes the person's name and is very short and simple, making it less secure.

Image: Display of three icons that depict different online platforms ranging from an email account to an online shopping account. There are also three different password examples, each one aligned to an ice. The first password is 4, asterisk, equal, uppercase M, lowercase k, exclamation, tilde, dollar sign, lowercase p. The second password is uppercase B, less than, plus, 3, lowercase g, 9, lowercase 9, lowercase w, closed bracket, backslash. The third password is pound, dollar sign, exclamation, uppercase B, lowercase j, hyphen, uppercase K, 2, 6, percent.

Narrator: Now that you know how to create a strong password, it's important that you use different passwords for every online account. If you only used one password for all of your accounts, then if someone guessed that one password, they could access your online banking, shopping, and email accounts just to name a few. As you can see, this person has created different passwords for all three of these accounts which makes it more challenging for a scammer to access her information.

Narrator: Another tip is to change your passwords often. This is especially important to do if you believe you have been the victim of a scam.

Narrator: If you follow the tips, we've mentioned so far in making unique and complicated passwords for each one of your online accounts you're probably wondering how to keep track of them all. Instead of writing them down on paper, you can store them securely online with a password manager that keeps track of your passwords for different sites. There are a number of password managers that are available for free or at a low cost. See the end of this tutorial for some examples of password managers that you might want to try.

Narrator: If you follow the tips, we've mentioned so far in making unique and complicated passwords for each one of your online accounts you're probably wondering how to keep track of them all. Instead of writing them down on paper, you can store them securely online with a password manager that keeps track of your passwords for different sites. There are a number of password managers that are available for free or at a low cost. See the end of this tutorial for some examples of password managers that you might want to try.

Narrator: To review, when creating passwords try to make them as difficult to guess as possible. You can do this by making them long, using both uppercase and lowercase letters as well as symbols and numbers. Even though it can be tempting to include personal information this makes it easier for hackers to guess your password.

Narrator: Some additional strategies are to make different passwords for every site and to change them frequently. And finally, try using a password manager to keep track of all of your strong passwords.

Image: Display of three different online password managers. The list includes, Last Pass, 1Password, and Google Chrome Password Manager.

Narrator: Here are some of the Password Manager resources mentioned earlier to help you remember your passwords, some are free, and some are low cost.

Narrator: We hope you found this video valuable. While optional, please take one minute to provide feedback on your experience, by clicking on the survey link that will display shortly. Thank you for joining and don't forget to check out the other Help@Hand videos.