Title: Tips for Staying Safe Online: Using Public WifI

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: Using Public Wi-Fi 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 4 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 talk about strategies for using public Wi-Fi networks to help protect your personal information.

Narrator: Wi-Fi is the name for wireless networks that help us to connect with the internet without using cables. We can have Wi-Fi in our homes and can also access free public networks that are known as Wi-Fi hotspots. You can find these hotspots in places like the library, coffee shops, hotels and airports.

Narrator: While it's certainly convenient to have access to Wi-Fi when you're out and about, it's important to know that most Wi-Fi hotspots do not have great security protections in place. By using an unsecure network, you can make yourself more vulnerable to strangers who might want access to your personal information. This type of person is referred to as a hacker and they have tools that can allow them to look at your private documents, contacts, and log in credentials. If they have this type of information, they can pretend to be you and scam people in your contact list. They can also get access to your online accounts including those that contain financial information.

Image: Display of a question that asks, What are some things I can do to protect myself when using public Wi-Fi?

Narrator: While it's always safest to use a secure Wi-Fi connection at home, there are some steps you can take to protect yourself when using public Wi-Fi. You can be careful about what you choose to do online and can also take steps to secure your computer against any potential cyber-attacks.

Narrator: Some wireless networks are more secure than others. When possible, you should connect to a Wi-Fi Protected Access, called WPA and WPA2 networks. WPA and WPA2 are encryption tools which means that they scramble the network connection so that no one can listen in and look at the websites you're visiting. Of the two types of networks, WPA2 is generally more secure and both types will require a password to log in.

Image: Display of a pop-out window that reads “The Wi-Fi network “admin2” requires a WPA2 password.” This window has a text box to enter a password and two check boxes below that read “Show Password” and “Remember this network” below these are two clickable buttons a “Cancel” button and a “Join” button.

Narrator: Here’s an example: When you select a Wi-Fi network from the available network options, you will be asked to enter a password. If you’re at a café or library or other place of business, they will often have a password for their network.

Narrator: Another strategy to use when accessing public Wi-Fi is to navigate to websites that have security protections in place. In addition to using a secure network, using websites that have taken some measures to protect you will make it harder for hackers to steal your information.

Narrator: Here is an overview of a few strategies you can use when you’re considering whether to visit a website. You can tell a lot from the website address which is also known as the URL. Look for a padlock and s after the “http” and double check that the website address is spelled correctly. If a website does not meet these criteria, consider avoiding it when using public Wi-Fi and at the very least do not enter any personal information. For more details on using secure websites, check out the Help@Hand webinar in our first series called “Safer Website Browsing”.

Narrator: When possible, try to do online shopping and banking from secure networks.

Narrator: If you’re using an unsecure network or website, a hacker might access your credit card information when you’re making an online purchase.

Narrator: And it’s even more important to avoid doing online banking when using a non-secure network as a hacker could access your bank account information.

Narrator: When using online accounts such as email or Facebook it’s often easier to remain logged in, however, this makes us more vulnerable to hackers.

Narrator: As a general practice, it’s best to log out of accounts after you’re done using them.
You can also take steps to protect your computers against cyberattacks when you’re using public Wi-Fi. One easy way to increase your level of protection is to keep your computer software up to date.

Narrator: Updating your computer software means that your computer will have the most recent security protections that are meant to stop viruses from harming your computer. Cyber criminals are constantly changing their strategies for accessing people’s information and so it’s important that you have the newest software in place to help protect you from these new threats.

Narrator: In addition to updating your computer software, you can also go a step further by downloading anti-virus and anti-malware software programs.

Narrator: Anti-virus software programs can protect against some of the older and more common computer viruses and anti-malware software protects against some of the newer threats. Check out the Help@Hand “downloading anti-virus and anti-malware software” webinar for more information.

Narrator: And finally, another tip is to always turn on your computer’s “firewall” to block attempts from strangers to destroy information on your computer.

Narrator: Your firewall stands between your computer and the internet. Its purpose is to provide a shield against hackers who are trying to access information on your computer.

Narrator: Usually you can find this setting within your computer’s “system preferences”.

Narrator: To protect your personal information, it’s important to keep these strategies in mind when using public Wi-Fi. When possible use a secure network, visit sites that have security protections in place, limit online shopping and banking and log out of your accounts when you’re not using them.

Narrator: You can also take steps to protect your computer by regularly updating you software, installing anti-virus and anti-malware protection and turning on your computer’s firewall. Check out the Help@Hand Downloading Anti-virus and Anti-Malware video for more information.

Narrator: We hope you found this video valuable. While optional, please take one minutes 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 the other Help@Hand videos.