Title: Tips for Staying Safe Online: Taking Action After a Scam or Malware Attack

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 Taking Action After a Scam or Malware Attack 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. This is course [4] in a 4 course series called Tips for Staying Safe Online. The videos in this series can be viewed in order or in any order based on your interest.

Narrator: Even when we try our best to identify safe websites and emails, we can still sometimes find ourselves victims of online scams or malware attacks. The following video will share some tips for what to do if this happens to you.

Narrator: An internet scam occurs when someone is tricked into sharing their personal information online which can include their credit card information, user login and passwords, and information related to their identity such as their name, social security number, and birthday.

Narrator: One way an internet scam can happen is through phishing, which are attempts to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity. This can occur through emails, websites, or ads that seem real on the surface.

Narrator: We can also accidentally download malware, a software which can cause damage to our computers and give others unauthorized access to capture personal data. This can occur through ads that pop up on your screen, fake websites or email links and attachments.

Narrator: One type of malware is called a virus because it can infect your computer to alter the way it operates and it is designed to spread to others.

Narrator: If you're worried that your personal information may have been accessed by a scammer or if you believe you may have downloaded malware, here are five things you can do to limit the damage and protect yourself in the future. If possible, it's best to follow through on all five of these steps to increase the chances that your information will stay safe.

Image: Slide of a presentation, the title reads "Tip #1" and the body text reads "Change Passwords" there is also an image of a pop-out box that allows a password change.

Narrator: If you believe you may have experienced a scam, it is a good idea to change all of your online account passwords. This will make it harder for the scammer to get into your email account, online banking and shopping websites.

Image: At the top of this slide thee is an image with a lock. In the body the test reads “Weak Password: Kate1/22/68” with a red “X” next to it and the next line of text read “Strong Password: T5%9Llf$4a!” with a green check mark next to it.

Narrator: In general, it’s best to create passwords that are long, complicated, have both numbers and letters, and that do not contain any personal information such as your name, birthdate, or address. As you can see here the first password isn’t that secure because it contains the person’s name and birthdate. The second password is much more secure because it is complicated, includes numbers, letters, and symbols and doesn’t contain any personal information. You can check out our tutorial “Creating and managing strong passwords” for more information on this topic

Narrator: Another thing you should do after a scam is to notify the three major credit bureaus that your accounts may have been accessed by a scammer. These include Experian, Equifax, and TransUnion. You should also ask that they set a fraud alert for your accounts.

Narrator: The third tip is to reach out to your bank and credit card companies to freeze your accounts to prevent others from making unauthorized charges.

Image: The slide is titled “Tip #4” with a line of text that reads “Update your computer software” and below this there is an example of a Mac computer pop-up window that reads “Software Update. An update is available for your Mac. macOS 10.14.1 Update. More info…”

Narrator: Here’s tip 4 - if you own a computer try updating your software in case your computer has been infected by malware or a virus. Updating your computer software means that your computer will have the most up-to-date protections that are meant to stop viruses from harming your computer.

Narrator: If you have not yet downloaded this type of software check out our “downloading anti-virus and anti-malware software” tutorial

Image: This slide has there different images switched out during the dialogue. The title reads “Tip #5” and the body text reads “Run a system scan” the first image shows a Norton anti-virus anti-malware software tool. The second image shows a Windows Antivirus software tool. The third image is of a pop-up window that reads” Full Scan. Scans your entire computer. We recommend that you run a full Scan immediately after installing the application. Note that this may take some time.” Underneath that text there is a clickable button that reads “Run scan” and at the bottom is an additional pop-up window that reads “Full Scan completed 1 day ago. 104,967 files scanned. 4 objects processed:4 deleted.” There is also a clickable line of text that reads “Detailed report.”]

Narrator: And finally, if you have anti-virus or anti-malware software already installed on your computer run a complete system scan to locate any suspicious software.

Narrator: Here’s a recap: when you think you’ve been scammed be sure to:

a. Change your passwords
b. Notify your credit bureaus

c. Contact your bank, and credit card companies
d. In summary, when you think you've been scammed be sure to:
e. Update your computer software
f. Run a system scam

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