

Title: Tips for Staying Safe online: Important Terms

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 Important Terms 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 [1] 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: The on-line world can connect us to loved ones, help us learn about our health, and access useful resources. Just like in real life, however, when you're going online it's important to be careful about who you share your information with and to take some additional steps to protect yourself from phishing attempts, malware, and viruses. In this important terms video we will review some definitions of online threats and provide an overview of the tutorials included within the "Tips for Staying Safe Online" web series.

Narrator: What kind of information should we protect?

Image: Displayed on screen are a Social Security Card displaying the card holders full name and social security number, an image depicting "Birthday", a section of a map meant to depict an "Address" and the bottom half of a check displaying persons account and routing number.]

Narrator: In general, it's important that we're careful about sharing our full name, date of birth, social security number, home address, and bank account number when we're online as not everyone can be trusted

Narrator: Phishing is an online attempt to obtain sensitive information such as your usernames, passwords, and credit card details. These attempts can happen through emails, websites or ads that all seem real on the surface.

Narrator: Another thing to watch out for is malware which can cause damage to your computer and give others access to your personal data. This can occur through ads that pop up on your screen, fake websites or email links and attachments.

Narrator: Viruses are one type of malware that you may have heard of. Viruses can infect your computer and then spread to others.

Narrator: Luckily, there are some things we can do to help protect ourselves from phishing attempts, malware, and viruses. The following brief tutorials in this series, including this one, will provide you with some strategies for keeping your information safe.

- a. Important Terms (The video you are currently watching)
- b. Safer website browsing
- c. Identifying phishing emails
- d. Taking action after a scam or malware attack
- e. It's important to remember that there's always a risk when using the internet, but by following these safety precautions you can reduce the likelihood of your information being accessed by strangers and feel more confident when going online.

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.