Transcript: How to protect yourself online.

Narrator: Let's imagine that your digital privacy is your house. Think about how your house is filled with the things you like, pictures, technology, your valuables, and it also has the things you want to keep private, like your underwear. Now, take a good look at this guy. Would you trust this guy in your house? No? Well, it's too late. He's in there already. Let's learn how to keep him outside.

Narrator: Let's discuss passwords. If your house is your digital privacy, your password is the lock on the front door. A good password keeps shady people out, and a bad one, well. Let's try a stronger password, something with letters, symbols and numbers. That's the ticket. Keep your password strong and never share it. You don't give strangers the key to your house, so don't give them the key to your online information.

Narrator: Shady people are going to try to trick their way into your digital home. What at first seemed safe, might not be as secure as you think. Make sure you read any URLs carefully. For instance, HTTP is not a secure URL. What you want to say is HTTPS. And remember, if you receive a suspicious email requesting personal information, such as a username or password, it's probably a shady dude trying to get one over you. Don't just give access to shady people.

Narrator: If connecting to public Wi-Fi, ensure that you're connecting to a safe host. If the Wi-Fi connection requires information, like your email address or phone number, consider using alternative details. And if you're going to use a public computer, like one at the library, make sure you log out. Don't just leave your front door wide open to anybody.

Narrator: Remember that your online security is your digital home, so keep it safe. If you see any scams out in the wild, make sure you report them to www.scamwatch.gov.au.