EPISODE 395

Think Before You Click

Stay Safe Online · Part 3

Full transcript · speaking practice · vocabulary review

Hi! I'm Georgiana, and I'm back with a new episode.

If you want the transcript, you can get it at SpeakEnglishPodcast.com.

By the way, I also teach private **English conversation classes**. **Would you like to practice speaking English with me**? Visit **SpeakEnglishPodcast.com** to learn more.

This is Part 3 of our series about staying safe online.

Sometimes a strange message is easy to notice. It looks wrong from the beginning.

But other messages are more believable because they mention something real: a purchase you made, an appointment you have, or a hotel you booked.

That is what happens to Elena.

Elena has a real hotel booking. A few days before her trip, she receives a message about it. The hotel's name is correct, and the page she opens looks familiar.

But familiar does not always mean **legitimate**.

Imagine someone wearing a hotel uniform. The uniform may look real, but that alone does not prove the person works at the hotel. A webpage can work the same way.

A **look-alike website** is made to look like a real website. The colors, name, and design may seem right, but the page belongs to someone else.

On this page, Elena is asked to download a file. She did not expect any file, so this **unexpected download** feels **suspicious**.

Elena booked a hotel room, not a mysterious piece of software.

The message also includes an **attachment**, which is a file sent with a message. But Elena does not open it. She stops before entering any information and decides to **take a second look**.

She wants to **verify** the message, but she does not use the contact information inside it. Instead, she opens the hotel app she normally uses and calls the saved hotel number. That app and number are a **trusted source** because Elena already knows where they came from.

The hotel tells her that her reservation is fine. It did not send the message or ask her to download anything.

The booking is real, but the message isn't.

So yes, this was **phishing**.

The file might contain **malware**, which is harmful software. Elena cannot know what is inside the file just by looking at its name. If she opens a harmful file, her device or information could become **compromised**.

This does not mean that every download is dangerous. It means that an unexpected request deserves a pause and a different way of checking.

And one quick note about a **security update**: real updates are important, but install them through your device's normal settings. Do not install one just because a strange message tells you to.

All right. Now let's practice with a Mini-Story.

Mini-Story

I will tell you a story by asking many easy questions. Answer aloud if you can. Short answers are perfect.

Elena was planning a trip.

Was Elena planning a trip?
Yes, she was. Elena was planning a trip.

Did she have a real hotel booking?
Yes. She had a real hotel booking.

Did she book a hotel room or an entire hotel?
A hotel room. She booked one room, not the entire hotel. She did not need three hundred bedrooms and a breakfast buffet all to herself.

A few days before the trip, Elena received a message.

Did the message talk about her hotel booking?
Yes, it did. It mentioned the hotel she had really booked.

Did that make the message seem believable?
Yes. The information was connected to something real in Elena's life.

Did Elena immediately know that the message was phishing?
No, she didn't. At first, the message looked normal.

Elena opened the page in the message.

Did the page look completely strange?
No. It looked familiar.

Was it the real hotel website?
No, it wasn't. It was a **look-alike website**.

Did a familiar design prove that the page was legitimate?
No. A familiar design did not prove anything.

Was the page a little like someone wearing a hotel uniform?
Yes. The uniform looked right, but it did not prove that the person worked there.

Then the page asked Elena to download something.

Did Elena expect a download?
No, she didn't. It was an **unexpected download**.

Did the page ask her to download a file, a hotel menu, or the entire hotel?
A file. It asked her to download a file. Fortunately, nobody tried to download the entire hotel. That would require a very large phone.

Was Elena expecting mysterious software with her room?
No. She had booked a room, not mysterious software.

The message also had an **attachment**.

Did Elena open the attachment?
No, she didn't. She did not open the file.

Did she enter her information on the page?
No. She stopped before entering anything.

Why did she stop?
Because the request was **suspicious**.

What did Elena decide to do?
She decided to **take a second look**.

Did she use information from the message to check the message?
No, she didn’t.

How did she verify it?
She opened the hotel app she normally used. Then she called the hotel using a number she had already saved.

Was the normal hotel app a trusted source?
Yes, it was. Elena already knew that the app was real.

What did the hotel tell her?
The hotel told her that her reservation was fine.

Had the hotel sent the message?
No, it hadn’t. The hotel did not send it.

Had the hotel asked Elena to download the file?
No. The hotel had not asked for any download.

So, was the hotel booking real?
Yes. The booking was real.

Was the message real?
No. The message wasn’t.

The booking is real, but the message isn’t.

Did Elena know for certain that the file contained malware?
No, she didn’t. She did not open it, so she did not know what was inside.

Could a harmful file leave her device or information compromised?
Yes, it could. That was why she did not take the chance.

What would Elena do if her phone needed a security update?
She would install it through the phone’s normal settings, not through a strange message.

Thanks for listening.

And I’ll see you in the next episode.

Review

Vocabulary from This Episode

Review the 12 key words and expressions before listening again.

01 **phishing** a trick that uses a false message or page to steal information.	07 **look-alike website** a false website designed to look like a real one.
02 **suspicious** making you think that something may be wrong.	08 **attachment** a file sent with a message or email.
03 **verify** check that something is real or true.	09 **unexpected download** a file that a page or message asks you to download when you were not expecting it.
04 **legitimate** real and official.	10 **malware** harmful software that can damage a device or steal information.
05 **take a second look** examine something again more carefully.	11 **trusted source** a person, app, website, or contact method you already know is reliable.
06 **compromised** no longer fully safe because someone may have access.	12 **security update** an official update that helps protect a device or program.

Continue your speaking practice

Build fluency with **guided audio lessons** and mini-stories.

Explore my Premium Courses >





Georgiana
Founder of Speak English Now Podcast
SpeakEnglishPodcast.com