Security Risks on Apps and Websites

Facilitation Guide

Help learners recognize and avoid different pitfalls and risks on apps and websites.

Overview

This module introduces learners to the various pitfalls and risks that can exist on apps and websites and helps learners better avoid these pitfalls.

For more information, be sure to watch Series 3 and Series 4 training videos from NYC Digital Safety.

Outcomes

By the end of this module, participants will be able to:

- Describe different pitfalls and risks on apps and websites
- Name strategies for avoiding pitfalls on apps and websites
- Identify methods for browsing the web safely

Format + Time Frame

This module provides an information overview of the various pitfalls and risks that can exist on apps and websites and shares methods for avoiding these pitfalls and for browsing the web safely.

This module will take approximately 30 to 35 minutes to complete. You can extend this module by combining this module with others on topics such as browser extensions or private browsing for a longer learning experience.

NYC Digital Safety
Privacy & Security

Materials

- Slide deck
- Facilitation guide
- Handout

Lesson Plan

Activity	Materials	Time Needed
Introduction and welcome Greet learners and review the plan for this module.	Slides 1 and 2	2 minutes
Defining security risks on sites and apps Share the handout with learners at any point during this lesson. Provide a brief overview of the types of pitfalls that can exist on websites and apps. Pause to see if anyone has anything else to add.	Slide 3	4 minutes
Pitfalls and risks on sites and apps Review some of the different pitfalls that exist on apps and websites, including malware, cookies, and trackers. Next, share some signs of a risky website or app. Pause to see if anyone has a question or anything else to add.	Slides 4 and 5	10 minutes

Ways to avoid risky sites and apps Review different strategies for avoiding risky apps and for avoiding risky websites, including using tools like secure browsers and developing a greater awareness of red flags and warning signs. See if anyone has other tips to add or share.	Slides 6 through 8	12 minutes
Wrap up, final tips, and final questions Review the closing thoughts and share the suggested resources. See if anyone has any final questions.	Slides 9 through 12	5 minutes

Considerations

This module emphasizes a range of risks and pitfalls that can exist on different apps and websites. Certain kinds of websites, such as places where people can pirate media, often carry more risks. You might consider being prepared in case these kinds of websites come up in conversation and consider how you might like to handle those conversations. One approach you might consider is noting that, regardless of someone's views on pirating sites (for example), it is important to be aware of the digital security risks and pitfalls they carry.

Options and Variations

This module pairs well with other modules about websites, browser extensions, and apps. You could consider either combining modules or running a whole workshop series on dealing with websites and apps and browsing the web safely.

You can also provide this information and content to patrons via a service point by sharing the guided handout with them.

Assessment

The following are some suggested assessment questions that you can use and adapt for your own purposes. These questions can help you assess various things, including knowledge retention, personal views and preferences, and concept application.

You might consider asking these as a pre or post test, or you can have learners answer these as part of an exit survey or a follow-up survey. Keep reading for suggested questions and an answer key with further details and explanations.

Questions for Participants

What are some risks that can exist on apps and websites?

A. They can contain malware
B. They might have poor data security practices
C. They might have login practices that aren't secure
D. All of the above

What should you not do in order to avoid risky apps or websites?

A. Be cautious with what you install or download
B. Make sure websites have "https" in the URL
C. Don't click links from unknown or suspicious sources
D. Visit the site and look around for suspicious signs

What is Safe Search?

A. An option in web browsers to filter and block explicit search results
B. A way to block scam websites
C. A way to block malware and viruses
D. A form of spell check

Answer Key

What are some risks that can exist on apps and websites?

Answer: D, All of the above

Problematic apps and websites can put your personal data at risk or expose you to malware.

What should you not do in order to avoid risky apps or websites?

Answer: D, Visit the site and look around for suspicious signs

Being cautious with what you download, click, or open is a good best practice for avoiding risky sites. Likewise, making sure sites have the more secure "https" protocol is important. Visiting a risky site isn't a good idea since that can expose you to malware.

What is Safe Search?

Answer: A, an option in web browsers to filter and block explicit search results

Safe Search is an option to filter explicit results, many of which contain other security risks or malware.

Connections to Other Modules

This module connects to many other modules. The following suggestions provide opportunities for exploration, connection, and potential programming. However, feel free to explore and make connections between other modules not listed here as well!

1.1 Phishing Schemes

2.1 Cookies

2.2 Private Browsing
2.2 Browser Extensions
2.2 Browser History

2.2 Ad Settings

3.2 Malware

4.2 Analyzing a URL

These and other modules can be found at this project's website, nycdigitalsafety.org.

About This Project

These materials were released in October 2022 as part of NYC Digital Safety: Privacy & Security.

NYC Digital Safety: Privacy & Security is a partnership between New York City's three library systems — Brooklyn Public Library, The New York Public Library, and Queens Library — and METRO Library Council. With support from the New York City Office of Technology and Innovation, this project ensures that NYC residents can rely on public libraries for their questions about internet privacy and security.

Visit nycdigitalsafety.org for more information.