NYC Digital Safety
Privacy & Security

Analyzing a URL

Facilitation Guide

Equip learners with the skills they need to analyze URLs and recognize signs of risky URLs.

Overview

This module helps learners better identify and understand different aspects of URLs, and equips learners with the skills they need to analyze URLs and to identify risky or unsafe URLs that should be avoided.

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

Outcomes

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

- Describe the different parts of a URL
- Use best practices for analyzing a URL
- Identify signs of unsafe URLs

Format + Time Frame

This module provides an information overview of the various parts of URLs and the signs of a risky or unsafe URL. This module will equip learners with techniques that they can use to better analyze and understand URLs they encounter.

This module will take approximately 50 minutes to complete and includes an activity and an opportunity for resource exploration. If you have less time, you could have learners do the activity or explore resources on their own later. You can also extend this module by combining it with others on topics such as avoiding various kinds of scams and schemes and risks such as malware.

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
Risks of malicious URLs Go through this list of potential risks and pause to see if anyone has anything else to add.	Slide 3	5 minutes
Parts of a URL Go through each highlighted portion of the URL and pause at the end to any questions.	Slides 4 through 6	7 minutes
Signs of a risky URL Go through this list of signs of a malicious URL and pause to see if anyone has anything to add or a question.	Slide 7	5 minutes
Activity: Analyzing a URL Put participants into small groups or pairs. Show them the two different examples (take about 5 minutes for each).	Slides 8 and 9, handout	10 minutes

Encourage them to discuss their thoughts and write down observations. Bring everyone together to discuss what they have seen. If you have additional time and want to extend the module, you can have participants review the handout together to get additional practice with analyzing URLs.		
Activity wrap-up Review the answers to the previous activity on this slide and make note of anything your learners didn’t cover or additional things they noticed.	Slides 10 and 11	5 minutes
Tactics used by scammers Go over the terms and examples on these two slides. Pause to see if anyone has anything else to add.	Slides 12 and 13	7 minutes
Avoiding risky URLs Review the suggestions listed on this slide and pause to see if anyone has any additional items to add to the list.	Slides 14 and 15	3 minutes
Wrap up, final tips, and final questions Review the final tips and resources listed here. If you have extra time, consider having participants visit some of the listed resources to explore them.	Slides 16 through 20	5 minutes

Leave time for any final questions or concluding thoughts.		

Considerations

Risky URLs are often a key component of various kinds of scams and schemes. Email phishing schemes, for instance, often encourage targets to click on links that prove unsafe. These unsafe URLs can end up infecting devices with things like malware or otherwise compromise someone's security and privacy. As such, this module can be considered an extension of numerous other modules that deal with scams, schemes, and malware. While the material here can be introduced on its own, it works best alongside other information about avoiding scams and schemes. Consider your overall approach and whether or not you might want to merge this module with others on scams and schemes, or whether you'd like to include this as part of a series of workshops focused on scams, schemes, and/or malware.

Note that depending on your audience, you might have individuals who learned things about "good" domain endings in school as part of modules on source evaluation. For instance, many students are taught that websites ending in ".gov" or ".edu" are more reliable than a ".com." While web domains could be a good starting place for this module, since it is already familiar to many, note that you might need to spend some time complicating domains and helping learners recognize that a ".edu" doesn't automatically equal safe and good. Malicious URLs unfortunately often use names and cues that people trust to manipulate them or conceal risky or unsafe URLs!

Options and Variations

As noted, this module can serve as a key component of other modules on scams and schemes (particularly email phishing), malware, and related topics. Depending on your overall goals and approach, there are a few variations that you might consider here. First, you could merge this module into other modules on schemes and scams. Second, you could provide learners with this handout if you are already running a longer module on schemes and scams. Third, you could include this module as part of a longer series on schemes, scams, and/or malware.

You can also provide this information and content to patrons via a service point by sharing the guided handout with them. Note that if you are providing people with handouts to peruse on their own, you might want to pair this one with a handout on phishing schemes or malware as a way to give people a better sense of where they might encounter risky URLs and when and why they might want to analyze URLs as a way to avoid things like malware and scams.

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

Which of the following is not a standard part of a URL?

A. Web protocol
B. A domain name
C. A file path
D. A tracking cookie

What is a sign of a risky or unsafe URL?

A. The URL uses "http" or unsecured web protocol
B. The URL has a spelling error
C. The URL contains hyphens and symbols
D. All of the above

What is not something that you should do to check for an unsafe link?

A. Hover over the link to see if it looks suspicious or unexpected

B. Use a URL extender to see the full version of a shortened URL

C. Click the URL and see if the website looks suspicious

D. Pay attention to things like spelling errors in the URL

Answer Key

Which of the following is not a standard part of a URL?

Answer: D, a tracking cookie

While tracking cookies can be a part of a URL, it isn't considered a key, standard aspect of one.

What is a sign of a risky or unsafe URL?

Answer: D, All of the above

Unsafe URLs often contain small spelling errors, hyphens or symbols, or lack the HTTPS secure protocol. They are designed to appear legitimate at first glance and, often, to mimic a known site such as Microsoft or Facebook.

What is not something that you should do to check for an unsafe link?

Answer: C, click the URL and see if the website looks suspicious

The key here is to look for visual clues or use a tool to check the URL in order to avoid clicking on it.

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

3.2 Identifying Email and Text Spam

3.2 Malware

3.2 Dealing with Scammers

3.2 Pitfalls on Apps and Websites

4.1 Avoiding Social Engineering

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.