NYC Digital Safety
Privacy & Security

Identifying Email and Text Spam

Learn how to recognize and deal with email and text spam.

1. How Can I Identify Email and Text Spam?

Email and text spam are often trying to get you to fall for a scam or a scheme, give away your personal information, or inadvertently put malware onto your device.

Here are some signs to keep in mind:

- Spelling and grammar errors
- Urgent messages trying to get your to rush or do something quickly
- Messages that ask you to download a file or click on a link
- Unexpected messages from unknown senders
- Offers of prizes or deals
- Requests for account information

Text and email spam often tries to impersonate a trusted business or a service that you use, such as FedEx or Apple. Be alert for errors, odd links, or weirdly urgent requests. Legitimate businesses don't request your personal information, for example.

2. Test Your Skills

To test out your skills, you'll first be reviewing examples of real phishing schemes and scams from the New York DMV:

- Visit this site: https://dmv.ny.gov/more-info/phishing-examples
- If you are in a workshop, your instructor might have samples prepared for you to review. If you are exploring on your own, you can work through some of the more recent examples on this website and see if you can identify the type of spam you are seeing.

Note your observations here:

Next, try to apply your knowledge and observation to your own accounts:

- Open up your email and visit your junk folder. See if you can identify examples of different kinds of spam messages that you might be receiving
- Next, look at your text messages and see if you can spot any examples of spam texts

Note your observations here:

Based on the examples you have seen, in your own accounts and via the examples provided, make a list of the common types of spam that you are seeing and their key identifying features.

Note your final thoughts and ideas here: