Lesson One/Hour One - Digital Citizenship - Email Scams and How to Recognize Them
Learning Target: Students will identify ways in which they can recognize and avoid email scams.

Purpose:
A few weeks ago, one of our accounts was hacked and an e-mail was sent out to everyone in our district from ... account. The e-mail included a link that brought users to a website that asked for private information. These types of e-mails are known as “phishing scams” and attempt to gain access to private information. It is important that we discuss e-mail scams like this to prevent possible attacks in the future.

Discussion Outline (10 min):
Define what “Phishing Scams” are to students.
Phishing Scams - The attempt at getting personal information from users online by posing as a legitimate company.

Explain that a few weeks ago, one of our school accounts was hacked and that we got a fraudulent e-mail from ... account that was an attempt at a phishing scam. Many times, emails containing viruses look very similar.

Ask students to discuss the following questions in groups or pairs.

1. Have you ever gotten an “e-mail scam” message?
2. What do you think are some signs of email scams? (you could even have them research this online if you have time and students know how to do this.)

Whole Group Discussion (30 min):
Discuss thoughts as a class and go over the following questions that might help students identify an e-mail scam. Give examples of what some of them look like by googling examples of phishing emails or showing them this website with actual examples http://www.it.cornell.edu/security/phishbowl.cfm . Demonstrate with the data projector.

- **Does this look suspicious?** If the email looks at all suspicious or out of the ordinary, there is a chance that it is a scam. Ask yourself the following questions:
  - Does it sound like something this person and/or company would usually send?
  - Is the email blank except for an attachment?
  - Are there spelling or grammar mistakes?
- **Is there an attachment you weren’t expecting?** Usually when someone is sending you an attachment, they tell you about it ahead of time. E-mail scams commonly have attachments that take you to an external link or that ask you to download something that may be a virus.
- **Are they asking for private information?** Legitimate companies will not ask you to give private information through an e-mail or unsecure connection. Many times phishing scams are trying to gain access to private information such as bank accounts, social security numbers, and passwords.

When in doubt, you can always **ask the person** or **call the company** to verify whether the e-mail was sent by them or not.

Test questions:

1. Phishing is an email scam that can attempt to collect personal information or infect your computer with a virus.
    a. True
    b. False
2. Misspellings in an email message are not a sign that you might be a victim of an attempted phishing scheme.
    a. True
    b. False
3. It is a good idea to try to open a link to an attachment, if you don't know who sent you the message.
    a. True
    b. False
4. You should always give out your personal information, to anyone who asks, regardless of whether or not you know them or why they want it.
    a. True
    b. False
5. You can always ask the person or call the company to verify whether or not they sent you an email that you have questions about.
    a. True
    b. False