13 **Spam + Phishing**

Introduction

Email has become an essential tool for communicating, which is why it is so popular with scammers, cybercriminals, and advertising companies. In order to protect ourselves from phishing scams and malware, it is essential that we learn how to safely manage our mail.

In this lesson, you will learn tips for **managing spam and email attachments**. In addition, you will learn how to **identify and avoid phishing scams**.

Spam

Spam is another term for **junk email** or **unwanted email advertisements**. Today, a majority of emails are spam. This is because it's easy and inexpensive for spammers to send an email to thousands of people at the same time, and they can do it anonymously, making anti-spam laws difficult to enforce. **Phishing scams** and **malware** are often included in spam, so it is important to be able to effectively manage the spam we receive in our inbox.

Tips for dealing with spam

Use a spam blocker. A spam blocker can greatly reduce the amount of spam that ends up in your inbox. Most online email services like Yahoo! or Gmail have built-in spam blockers. You can also use a separate anti-spam program such as MailWasher, which can be used with Outlook or any other email program. Unfortunately, even with a spam blocker, some spam may still get through.

- **Don't reply to spam.** You may be tempted to reply to a spam email or click on a link within the email to unsubscribe. This may work with legitimate emails that you have subscribed to; however, spammers will rarely honor these requests. In fact, by replying or clicking a link, you are confirming to the spammer that your email address works, which means you may end up getting more spam.

- **Turn off images.** An email can contain images spammers can track. When you open the email, the images will load, and the spammer will be able to tell that your email address works, possibly resulting in even more spam.

- **Turn off your preview pane** (if your email service has one). You cannot avoid viewing spam when your email automatically displays it in your preview pane. Once you view a spam message, it may actually lead to receiving more spam. Therefore, you will need to weigh the convenience of using your preview pane with your desire to avoid spam.

Regularly check your spam folder. Sometimes spam blockers block legitimate emails. It's a good idea to regularly check your spam folder to make sure you are not missing important emails. Check your email program for settings that will allow legitimate emails that are being blocked

Email scams

Many spam emails aren't trying to sell you something—they're trying to steal your money or personal information. **Email scams** come in many different forms, but generally they work by promising you something that's too good to be true or by making you think something bad will happen if you do not act. Popular email scams include **work-at-home offers, weight-loss claims, debt-relief programs**, and **cure-all products**.

Advance-fee fraud

Have you ever seen an email or classified ad (for example, on Craigslist) promising you something if you advance a certain amount of money? The word for this is **advance-fee fraud**. It's different from other email scams because it involves corresponding with an actual person—someone who is trying to trick or mislead you by sharing their "personal story," which is almost always false.
One of the most notorious examples of advance-fee fraud is the **Nigerian letter scam**. To learn more, read this article from the Better Business Bureau: The Nigerian Prince: Old Scam, New Twist.

Phishing

View Video: ***Avoiding Spam and Phishing***

Phishing is a type of scam in which an email pretends to be from a bank or another trusted source in order to trick you into handing over your personal information. Scammers can use this information to withdraw money from your bank account or steal your identity. A phishing email will often have a **sense of urgency**. For example, it may claim that "unauthorized charges"

Additional tips and resources

- **Don't follow the link.** It's easy for an email to use the logo from a legitimate company in order to look "official," but any link you click could take you to a shady site. Always type in the web address or click on one of your own bookmarks to go to your bank or other trusted websites.
- **Report scams and spam.** Some email service providers have a "This is Spam" button or another method for reporting spam. You can also contact the company being misrepresented and report the spam. Another option is to email a report of the spam to the Federal Trade Commission at spam@uce.gov.
- **Get more information** and learn about **specific scams** by visiting New Email Scams - The Canadian Anti-Fraud Centre.

Dealing with email attachments

Email attachments are especially dangerous because they can contain viruses and other malware. When you open the attachment, the malware can be automatically installed on your computer, and you may not even realize that anything has happened. Malware can damage files on your computer, steal your passwords, or spy on you, so it's important to be extra careful when you receive attachments.

Tips for dealing with attachments:

- **Don't open any attachment that you weren't expecting.** Even if an email looks like it's from someone you know, it may have been automatically sent to you by a virus. That's how many email viruses spread. If you receive an attachment from a friend, you should call or email that person to verify that the email was meant for you.
- **Keep your antivirus software updated.** Viruses can spread quickly, and if your antivirus software isn't up-to-date it may not be able to block new viruses.
- **Keep your computer's firewall on.** Firewall software helps to prevent people or malware from gaining access to your computer through the Internet.
- **Scan attachments for viruses before downloading.** Many online email providers can scan attachments for viruses, and some will not let you download any attachment without scanning it.