PHISHING for SPAM

What's the difference and why does it matter?

Are you constantly getting useless mail that clutters up your inbox? Is it hard to find the email you actually care about?

We get offers for travel deals, cheap pharmaceuticals, singles in your local area, and more get-rich-quick schemes than you can shake a stick at. Many of us receive unsolicited advertisements and "coupons" in email inbox every week. Spam has been around longer than email and while it's annoying, it's still pretty easy to deal with.

However, modern technology has taken things to a new level and it's important to understand what you could encounter with modern spam.

Spam?

First of all, let's be really clear on what spam is. Spam is a kind of unsolicited message that's sent out to a massive number of people and is often sent repeatedly. Usually this kind of advertising is unlikely to sway most people, but in large volumes they can usually count on catching someone.

Email spam is the most common because of the low cost of sending out millions of messages. We also see SMS spam (mobile texts) that target as many phones as possible, as well as spam on social media sites.

Usually the messages offer some sort of scam service, but sometimes it can be a lot more serious.

Gone Phishing

Many spam emails will feature a link or attachment that they are trying to get you to click. This is fairly common in any kind of email advertising, but it could also be a phish.

Phishing is when someone is trying to trick you into downloading a virus or providing confidential information.

Have you seen an email telling you that you owe money to the CRA? Or something offering great deals through a strange link? These are all great examples.

Now, phishing is usually sent as spam because it means that they'll usually catch at least someone with a relatively low effort. Phishing isn't always so low effort though.

Spearphishing is a directed kind of phishing that's tailored toward a particular group or organisation. They'll use a bit of research to create messages that their targets are likely to trust.

Whaling is when phishing messages are uniquely tailored toward high value targets. This could be an IT administrator, an executive or a politician. Anyone who has power and access to what the cybercriminal wants.

How to Protect Ourselves

Neither of these tailored approaches are spam, so they are a lot harder to spot. Luckily, there are some tricks to keeping yourself safe from these threats.

- **Hover over links before you click**. Check to see if they are sending you to a legitimate site. Read the URL address and if it's full of strange numbers and letters, it's usually best to avoid it.
- **Scan attachments.** Before opening any attachments, scan them before you open them. Viruses can be hidden in almost any kind of file.
- **Watch before you log-in**. If the link takes you to a log-in page. Be extra careful that this is the real site. Sometimes criminals will link you to a fake site that will steal your login information.
- **Don't enable document macros.** Document macros can hide viruses. The best policy is to avoid enabling any document macros that you receive over the internet.
- **If you aren't sure, talk to the person offline.** When things seem fishy, the best approach is to check through another source. Call a trusted phone number or talk to them in person.