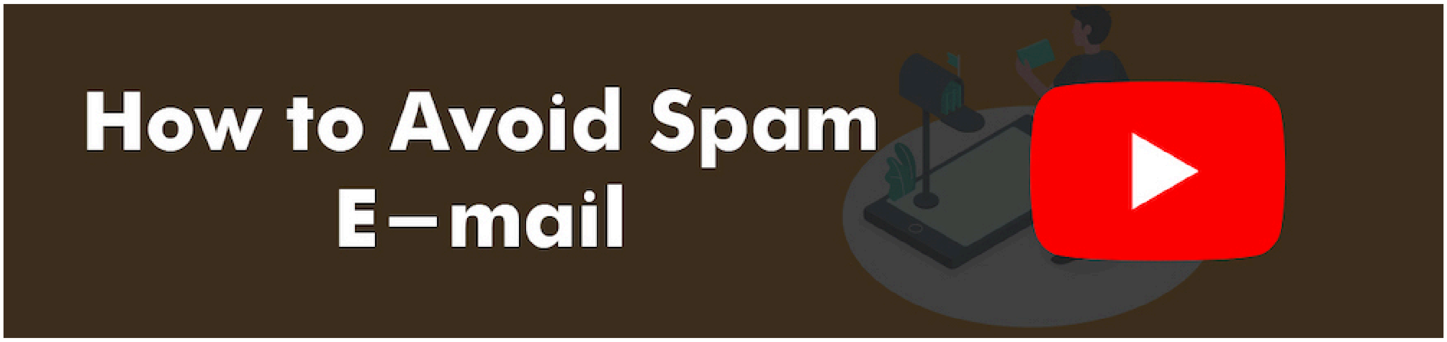
E-Mail Spam



Who?

Short Answer: Anyone

Long Answer: Spam E-Mails are sent out all the time and can go to anyone.

What?

Short Answer: Unsolicited Junk Mail

Long Answer: Email is both an excellent communication tool and also a way that companies can inform you about their latest products and services. However, email is frequently used to deliver unwanted material which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself.

These include the following:

Spam (or Junk) email

The vast majority of email sent every day is unsolicited junk mail. Examples include

- Advertising, for example online pharmacies, pornography, dating, gambling.
- Get rich quick and work from home schemes.
- Hoax virus warnings.
- Hoax charity appeals.
- Chain emails which encourage you to forward them to multiple contacts (often to bring ‘good luck’).

When?

Short Answer: Anytime

Long Answer: Spam can come at any point, if it does, just delete it.

Where?

Short Answer: E-Mails

Long Answer: Spam E-Mail can go to your work email, personal email, a friends email, etc.

Why?

Short Answer: To Gain Sensitive Information

Long Answer: Attackers usually want to steal something from you for some sort of gain, usually financial. They'll steal your Social to masquerade as you and buy things on your credit, they'll steal passwords to get into your bank account and transfer money out, and they'll steal much more if you're not careful.

How?

Short Answer: Don't open emails like this, just delete it.

Long Answer: Spam emails may feature some of the following warning signs:

- You don’t know the sender.
- Contains misspellings (for example ‘p0rn’ with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example “Buy now and get 50% off”).
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files.

Tips to protect yourself from spam emails

- Do not open emails which you suspect to be as spam.
- Do not open attachments from unknown sources.
  - Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.
  - Do not respond to emails from unknown sources.
  - Do not make purchases or charity donations in response to spam email.
  - When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails.
  - Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.
  - Most Microsoft and other email clients come with spam filtering as standard. Ensure yours is switched on.
  - Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.
- When choosing a web mail account such as Gmail, Hotmail and Yahoo! make sure you select one that includes spam filtering and that it remains switched on.