**What is Spam and Phishing and Why You Receiving These Emails**

You might know these emails by laymen’s terms such as “spam” or “junk mail”. Or better yet, the infamous “Nigerian Prince” scam email and even ads for questionable “miracle pills”. For the record we are talking about spam emails, not spam but food. Everyone who uses email has stumbled upon spam email messages. Yet, what is spam exactly? Where do these weird spam emails come from and why? Learn more about how spam email works and how you can stop receiving them.

**What Is Spam**

Spam is unwanted, unsolicited messages that are sent out in bulk. It is not limited to emails and includes text messages, phone calls, or social media. Regardless of the medium, spam is always unwanted and unrequested. The etymology of the word “spam” is actually in reference to a [Monty Python](https://www.youtube.com/watch?v=_bW4vEo1F4E) skit. In this skit, a group of diners is forced to eat spam regardless of whether they want to or not.

*Spam is NOT Email Marketing*

Many individuals sign up for newsletters, promotions or other subscriptions. While it can be annoying to receive these messages, this is not considered spam. If you change your mind on email marketing newsletters and promotions, you always have the option to unsubscribe or opt-out. Spam email and phishing will always be invasive and obnoxious.

**The Origin of Spam Emails**

[Spam](https://www.internetsociety.org/resources/doc/2014/what-is-spam/) has been around for quite some time and its origins can be traced back to the beginnings of email. The early email system was created with little to know security considerations. This made room for loopholes for spam to be sent easily and readily. In the 1990s, spammers realized that they could forge addresses and domains, when than lead to IPs getting blocked. However, this did not deter spammers. They ended up sending their messages through third party servers.

In the 1990’s domains became accessible and spammers were able to purchase entire domains. Eventually, hackers were able to develop malware to send via email. This malware was then inserted onto individual computers which created vast botnets.

<https://www.youtube.com/watch?v=NI37JI7KnSc>

**Why You Keep Getting Spam Emails**

“How do spammers find my email address?” is a question that perplexes a lot of people. Unfortunately, the truth is, companies receive compensation by selling your contact information to third-party companies. Spammers also use “spoofing” to hide their identity from internet providers and recipients.

Spam is cheap, which is what makes it so attractive to use. It costs pennies on the dollar to blast a bunk amount of emails. Also, if they even get a few favorable responses, the spammer will see a decent return on investment.

**Spambots and Spam Email**

The senders of email spam work with a multitude of email addresses. Email addresses are harvested by [spambots](https://en.wikipedia.org/wiki/Spambot), who scan website pages and social media profiles. These spam bots are web crawlers that are able to gather this information in the first place. Since email addresses have a simple and recognizable format, it is easy to code a spambot. When spammers grow a big enough database, they will send out spam emails in bulk.

It’s important to note that spammers don’t necessarily use bots for collecting email addresses. Sometimes they purchase email lists or obtain them from the dark web. Sometimes, they get these emails from hacking a company database.

If your website has CAPTCHA set up on forms and sign up pages, this will deter spambots from creating accounts on your website.

**What Is the Difference Between Spam and Phishing?**

Spam and Phishing emails are both unwanted and unsolicited messages. However, the difference between the two lies within the goal of the sender. Spammers (usually) are not trying to extract personal data or information. Rather, they are simply peddling unwanted goods and services.

On the other hand, Phishers are legitimate cybercriminals. Their goal is to get unsuspecting victims to give up personal information. This can be done through either deception or by sneaking malware onto your computer. It is similar to spam, where messages are often sent in bulk. However, their intention is to involve fraud, theft, stealing personal information.

**Types of Spam**

In 2021, spam has become a very diverse category, coming in many forms. As a rule of thumb, if you don’t recognize the sender, it is most likely spam.

<https://www.youtube.com/watch?v=zflsg6TRuos>

**Commercial Advertisements**

These are the most common types of spam. You’ve seen spam emails peddling everything from miracle cures, dating and adult content, financial opportunities or claims that you “won” a contest or sweepstakes.

**False and Misleading Information in Email**

A lot of spam emails contain false or misleading information with the intention of causing you to act out of urgency. Earlier this year, we had several clients come forward with emails from a law firm who were “[copyright trolls](https://faceless.marketing/higbee-associates-copyright-trolls/)”. They sent aggressive letters to businesses accusing them of copyright infringement and demanded a large sum of payment as compensation. These letters are not legitimate in any way, but are crafted to trick business owners into thinking that they have broken a law.

**Tech Support Scams**

This type of spam tries to convince the recipient that you have a technical problem that needs to be resolved. This email will suggest you contact a tech support team by responding to the email, or calling a phone number. These spammers will try to mask themselves as a legitimate tech company like [Apple](https://www.apple.com/) or [Microsoft](https://www.microsoft.com/en-us/).

**Phishing Emails**

Phishing emails are among the most dangerous types of spam. It is used by cybercriminals to trick recipients into giving up vulnerable information. Phishers are after valuable information such as logins, credit card information or personal information. (See below on how you can protect yourself against phishing attacks).

**Other Forms Of Spam**

* Comment Spam – Found on Website comment sections.
* Finance Spam - advertises loan options, stocks or mortgages
* Educational Spam – advertising online courses, seminars or degrees

**Notice the Signs of Phishing**

Learn what the signs of phishing are. By protecting yourself against phishing, you can avoid an attack. There are a few signs that a spam email is actually a phishing attempt.

* **Email Addresses** – The senders email address is usually a dead giveaway. Their email address should match the company that they represent. For instance, if you receive an email from [alan20230923@gmail.com](mailto:alan20230923@gmail.com) , it doesn’t match the company’s domain name. Also, look out for fake company emails like [support@Amazon1.com](mailto:support@Amazon1.com). Notice how it doesn’t show the proper domain of amazon.com.
* **Spelling/Grammar/Punctuation Errors** – An email from a legitimate company will contain the occasional spelling or grammar error. However, if you notice an unusual amount of spelling, grammar and even punctuation errors, that is a huge red flag.
* **Links** – If you suspect that the message that you received is phishing, do NOT click on the links under any circumstances.
* **Email Attachments** – Unless you are expecting an attachment, there is no reason why you should be opening one. You should not be opening email attachments from senders that you are not familiar with. If you do, make sure to scan the files using anti-malware software.
* **Sense of Urgency** – Dangerous phishing emails will contain a sense of urgency that makes you want to “act now”, and the language will convey this.

**What You Can Do To Prevent Spam**

Spam emails are annoying but they also pose a security threat if it includes phishing. Many people assume that they are savvy enough to spot spam messages. However, spammers have upgraded their methods in 2021 and have become more sophisticated.

* Sign up for forms using a “throwaway” account. – Many online companies and eCommerce platforms still require you to register for accounts using email addresses. Fortunately, you can use a “throwaway” disposable email address to filter out emails without it clogging your main email or work email.
* Do not engage with spam – Engaging in spam will lead the sender to believe that you are receptive. Do not engage with spam at all – do not download attachments, click links or respond to the sender.
* Mark emails as “spam” – If you see an unwanted spam email, make sure to check it of as “spam.” Every email client has a button that you can select to mark an email as “spam”. You are actually “training” your email client to get better at registering unwanted spam emails.
* Mark emails as “not spam” – Every now and then, make sure you are making legitimate emails as “not spam”. This will help your email client filter out spam for you.

**Take Control of Your Email**

Email and digital communication essential for businesses in 2021. We want to make sure that our clients and prospective clients to be able to do business via email without the threat of a phishing attack. Your company emails contain sensitive data and valuable information. It’s more essential than ever to protect your company, as well as make sure that your inbox is free of spam.

[*Faceless Marketing*](https://www.faceless.marketing/) *is the marketing firm that you can depend on to give you the best results and greatest return on investment (ROI). Reach out to Faceless for some consultation. Get a* [*FREE quote*](https://faceless.marketing/quote-request/)*on any of our services from printing to web design and SEO.*[*Call 1-800-357-1299*](tel:18003571299)*or Shoot us a*[*Message Here*](mailto:info@faceless.marketing)*.*