What is a SPAM

Why is it called spam?

The origin of the term “spam” for invasive bulk messaging refers to a Monty Python skit. In it, a group of diners (clad in Viking costumes) loudly and repeatedly proclaim that everyone must eat Spam — whether they want it or not. It’s similar to how an email spammer floods your inbox with unwanted messages.

When spelled with a capital “S,” *Spam* refers to the canned pork product that the above-mentioned Vikings love. Spelled with a lower-case “s” and *spam* means the unsolicited, disruptive emails and other messages that flood your inbox and other feeds.

Types of Spam

Spam can range from annoying emails to different types of internet spam, like social media comments full of excessive links or even sensationalist headlines in media outlets and on other websites that you can’t seem to *not* see.

Here are the main types of spam you can find online:

Spam emails

Spam emails are the most common type of spam you’re likely to encounter online. They clog up your inbox and distract you from the emails you actually want to read. Thankfully, most email clients allow you to report, filter, and block most spam emails.

SEO spam

Also known as “spamdexing,” SEO spam refers to the manipulation of search engine optimization (SEO) methods to improve the rankings of a spammer’s website in search

engines. We can divide SEO spam into two broad categories:

Content spam

Some spammers cram their pages full of popular keywords to try and rank the pages of their website higher when people make searches with those keywords. Others will use existing content without permission to make their own pages seem more substantial and unique.

Link spam

If you've come across a blog comment or forum post that's filled with irrelevant links, you've encountered link spam. The spammer is trying to exploit an SEO mechanic known as "backlinking" to drive traffic to their page.

Social media spam

With the rise of social media, spammers have been quick to take advantage of all the attention on those platforms, spreading their spam via bots and other sketchy accounts. Most social media spam contains links to commercial pages, which aim to increase traffic or revenue for a spammer's website.

Spam text messages and spam calls

Some spammers send text messages (SMS), push notifications, or even call your cell phone to get your attention. Spam messages can also take the form of instant messages via popular messaging apps like WhatsApp, Skype, and Snapchat. It's best to block spam texts and calls from suspected spammers, not answer weird texts, and never click links on any spam messages.

Tech support scams

Tech support scams usually begin with a phone call from someone pretending to be an IT professional from a legitimate company. The scammer will try to convince you there's

something wrong with your computer and that if you give them remote access they can fix it. Tech support scams can also start with malicious advertisements on infected sites.

Current events scams

The deluge of sensationalist news published daily gives spammers the opportunity to exploit headlines to capitalize on tragedies or political events. You might receive a spam message or spam email asking you to contribute to a fundraising campaign that isn't legitimate.

Malware spam (malspam)

Malware spam is exactly what it sounds like: spam that includes malware. It's usually delivered to your computer or mobile device via a spam text message or spam email. This type of spam can deliver almost any type of malware, from ransomware to trojans to spyware.

How to recognize spam

You can often recognize spam by its apparent urgency, commercial aims, and the unrealistic or exaggerated promises included in the message. Regardless of how it reaches you — via email, text message, social media, or a phone call — most spam fits into one of a handful of genres.

Spamming vs Phishing

The difference between spamming and phishing lies in the intent of the spammer (or phisher). Spammers are a nuisance, but they usually aren't out to hurt you. Phishing attacks, on the other hand, are carried out by cybercriminals who want to access your personal information or infect your device with malware.

Spammers have something to sell, and they've decided that spamming is an effective technique for promoting their product or service — of course, some products and services may be low quality or fraudulent. And while phishing attacks that cast a wide net are a type of spam, they usually have more nefarious goals — such as fraud, identity theft, and even corporate espionage.

The email shown below is an example of the infamous advance-fee “Nigerian prince” phishing scam. A browser with anti-phishing technology, such as Avast Secure Browser, can protect you against this type of scam.

Why am I getting spammed?

You receive spam messages because many companies sell their customers’ email address and other contact info to advertisers and other third parties. And spammers send bulk emails because it’s cheap. If only a handful of recipients respond to their spam campaign, the spammer will likely see a positive return.

Because most spammers use spoofing to conceal their identity from recipients and internet service providers, it’s difficult to hold them accountable. The low risk and cost of spamming make it an attractive option for less-scrupulous advertisers and marketers.

The problem of selling data to spammers was getting so bad that in 2018, the EU passed the General Data Protection Regulation (GDPR), a series of rules aimed at limiting what companies are allowed to do with their customers’ personal data.

By 2021, many companies had shifted away from third-party data processing, opting instead to keep customer data in house — reducing spam and increasing consumer privacy.

How to prevent spam

You can block spam with a few simple tips and tricks. Here are a few ways to prevent spam emails and avoid other spam messages:

- **Use the spam-reporting function.** Most email providers have an option (button) to report an email as spam. By reporting spam in your email, you can “train” your inbox to get better at detecting spam. Any spam emails detected will be sent straight to your spam folder. If your email client isn’t auto-detecting spam and phishing emails, switch to one that does.
- **Mark which emails are not spam.** Every so often, look at your spam folder, because sometimes legitimate messages end up there. If you find anything in your

spam folder that doesn't belong, move it to your inbox. That also helps train your spam filter to learn which emails to block and which to let through.

- **Sign up for some services with alternate email addresses.** Lots of ecommerce platforms and internet services require an email address. If it's not absolutely necessary, don't use your primary email for throwaway or one-time signups.
- **Don't interact with spam.** When you receive spam emails or text messages, don't click links, don't download attachments, and never respond to the spammer. If you do, they may think you're a receptive target — meaning that they'll send you more spam. Or the links may be infected or redirect you to fraudulent websites.
- **Don't publish your contact information.** Spammers can — and do — find contacts online. Keep your online presence as private as possible. This also extends to your phone number, physical address, and other personal information. Check out our guide to hiding your IP address online.
- **Check for data leaks involving your email.** Pop over to our free Hack Check tool and see if your passwords have leaked. If so, follow the instructions sent to your email to change your passwords and start removing your personal information from the web.
- **If someone you know sent you spam, tell them.** If you've received a spam message from a trusted contact, tell them that their account has been hacked and used for spamming. That way, they can take corrective measures and regain control.
- **Use updated software and strong security measures.** Keep your devices, software, and apps updated to protect yourself from spammers looking to exploit vulnerabilities. Use strong passwords for all your accounts and two-factor authentication when signing in to secure portals.
- **Use strong security software.**With spam and other online risks continuing to threaten your security, you need a strong antivirus app that gives you real-time protection against the assortment of threat vectors out there.