

# Avoid Spam

The majority of Internet-based scams start off with an unsolicited email. Whether it is a phishing attempt, a bogus lottery prize award notification, a fictitious greetings card scam, or someone from Nigeria with \$50,000 to give away, your inbox is where it all begins. Apart from being a general nuisance, unsolicited commercial emails, or spam, can cost you dearly if you are not careful online.

The best way to avoid the scam is to avoid the spam. Here are 10 tips for reducing the amount of spam that you receive:

1. Consider creating a free, web-based email account for use with anyone other than your close friends and family. Activate any junk mail filters that are provided, and use the account for online purchases and subscriptions. Delete the account and get another when spam levels get too high.
2. Choose a long email address that is difficult to auto-generate. Many spammers use 'dictionary' software to generate thousands of usernames that are then attached to the domain names of popular email providers, such as Hotmail, Yahoo, AOL and MSN. The longer your username (the portion of the email address before the @ symbol), the harder it will be for a computer to auto-generate.
3. Never disclose your email address on internet websites, blogs, discussion groups, forums or newsgroups - spammers routinely 'harvest' email addresses from the internet using automated software, or 'bots', and will capture your email address within hours.
4. If you must disclose your email address (for example, on your own website) consider embedding the address within an image/graphic file, thereby avoiding detection by email harvesting bots.
5. Never, never, never click the 'unsubscribe' link on unsolicited emails - this merely serves to authenticate your email address to spammers and is guaranteed to increase, rather than decrease the amount of spam that you receive.

6. Users of Outlook Express should consider blocking images in HTML email. Spam often contains images that act as 'web beacons' that notify the sender's web server when you preview or read email messages. This serves to validate your email address as being live and active, and will likely result in increased spam. Images can be turned off in Outlook Express by going to Tools > Options > Security Tab > "Block images and other external content in HTML e-mail".
7. Uncheck '3rd party' disclosure boxes when making online purchases or subscribing to online services - they are often checked by default.
8. Do not assume that the owners of a website are always telling the truth when they promise that they will never pass your email address to others. Such promises are incapable of being validated, and it will be impossible to trace any breach to the perpetrator responsible. Be an Internet sceptic.
9. Remember what you sign-up for. Keep confirmation e-mails in a separate email folder so that you can easily distinguish spam from genuine emails.
10. Never click on links within emails, regardless of their nature. Doing so will not only validate your address to the sender, but may also direct you to a phishing website or to one which will launch malicious code on your PC. At the very least, it will elevate you, the recipient, to the unenviable status of 'gullible', and the frequency and malevolence of the spam you receive will increase.

All our alerts are available in a range of formats and languages, including large print. Please contact Cath Wohlers if this would be helpful to you, or to someone you know.

Email: [cath.wohlers@staffordshire.gov.uk](mailto:cath.wohlers@staffordshire.gov.uk)  
Address: 14 Martin Street, Stafford, ST16 2LG