

PLEASE DO NOT REPLY TO THIS MESSAGE.

If you or someone you know is vulnerable and has been a victim of fraud, please call Essex Police on 101.

Report fraud or attempted fraud by contacting Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

AMAZON BRUSHING – BRUSH UP ON HOW TO PROTECT YOURSELF

Have you received an Amazon parcel recently that you have not requested? Amazon 'brushing' scams have surfaced over the last three years and centre around Amazon sellers being able to leave fake positive reviews for their items.

How does it work?

A third party seller will get the name and address of a consumer. They will then purchase an item and send it to the unsuspecting person, claiming on Amazon that it is a 'gift'. This allows that seller to leave a fake review for that item, even though someone else has received it. As a result, they can improve their Amazon seller rating which will encourage other customers to shop with them. Also, the amount of times a product has been sold will improve its chances of appearing in other customers searches, which is another benefit to the seller.

Should I be worried?

Most people who receive these items are not charged for them. The main concern is how the seller obtained the person's name and address in the first place. Sometimes this information is readily available on an internet search, other times it might be the result of a data breach.

A good way to check whether your data has been compromised is to use the site www.havebeenpwned.com. By entering your email address, you can see if/when it was involved in any data breaches and where these occurred. If this is the case, then it is essential that you change your password using the National Cyber Security Centre guidance below.

'Tell2, protect many' is a communication initiative that empowers you to spread crime prevention messages to others in your life, who otherwise may never know. Start with 'tell2' and ask them to do the same. It starts with YOU!

What should I do if I've received a parcel?

If you do receive a parcel you have not requested, immediately notify the retailer. Use information available from Amazon or the retailer's website rather than information provided in any email correspondence, in case this is also part of the scam. Then, change your password using the below advice and report to Action Fraud. You could also monitor your bank account to ensure there is no suspicious activity in the coming weeks.

Whilst free items may be an unexpected surprise – **if it's too good to be true, it usually is!**



Using passwords To protect your devices & data

Passwords are an effective way to control access to your data, the devices you store it on, and the online services you use. This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen. For more information, please refer to www.cyberaware.gov.uk.



Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If successful, they will use this **same password** to try and access your **other accounts**.

Criminals also try and trick people into revealing their passwords by creating fake 'phishing' emails that **link to dodgy websites**, or by using **persuasive techniques** through social media.

Even if you look after your passwords, they can still be stolen if an organisation containing your details suffers a **data breach**. Criminals will use these stolen customer details (such as user names and passwords) to try and access other systems.

© Crown Copyright 2020

Create strong passwords

Create a strong and memorable password for your email account (and other important accounts).



Avoid using predictable passwords (such as **dates, family and pet names**). Avoid the most common passwords that criminals can easily guess (like 'passw0rd').



Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to (for example) your banking account.



To create a **memorable password** that's also hard for someone else to guess, you can **combine three random words** to create a single password (for example *cupfishbiro*).

Look after your passwords

If you store your passwords somewhere safe, you won't have to remember them. This allows you to use unique, strong passwords for all your important accounts.



You can write your password down to remember it, but **keep it somewhere safe**, out of sight, and (most importantly) **away from your computer**.



Most web browsers will offer to store your online passwords. **It's safe to do this**. Browsers will also detect 'dodgy' websites that phishing emails try and trick you into visiting.



You can also use a standalone **password manager** app to help you create and store strong passwords.

Use 2FA to protect your account

Many companies allow you to set up two-factor authentication (also known as 2FA) on your accounts. It's called 2FA because it involves signing into your account using **two passwords or codes**; one that you know, and the other usually sent to your phone.



The most common form of 2FA is when a code is sent to your smartphone that you must enter in order to proceed. You should **set up 2FA for important websites** like banking and email.



Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA.

The website www.telesign.com/turnon2fa/ contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

TURN IT ON

What to do if your password is stolen?

If you suspect your password has been stolen, you should change it as soon as possible.



If you have used the same password on any other accounts, change these as well.



You can use the website www.havebeenpwned.com to check if your information has ever been made public in a major data breach.

www.ncsc.gov.uk [@NCSC](https://twitter.com/NCSC) National Cyber Security Centre [@cyberhq](https://www.instagram.com/cyberhq)

'Tell2, protect many' is a communication initiative that empowers you to spread crime prevention messages to others in your life, who otherwise may never know. Start with 'tell2' and ask them to do the same. It starts with YOU!