Protect yourself from online fraud: Signs you may be compromised

Britons have been told of five tell-tale signs their internet security may have been compromised.

Experts have issued a warning urging Brits to take their online security seriously, as criminals look to exploit insecure profiles and personal information.

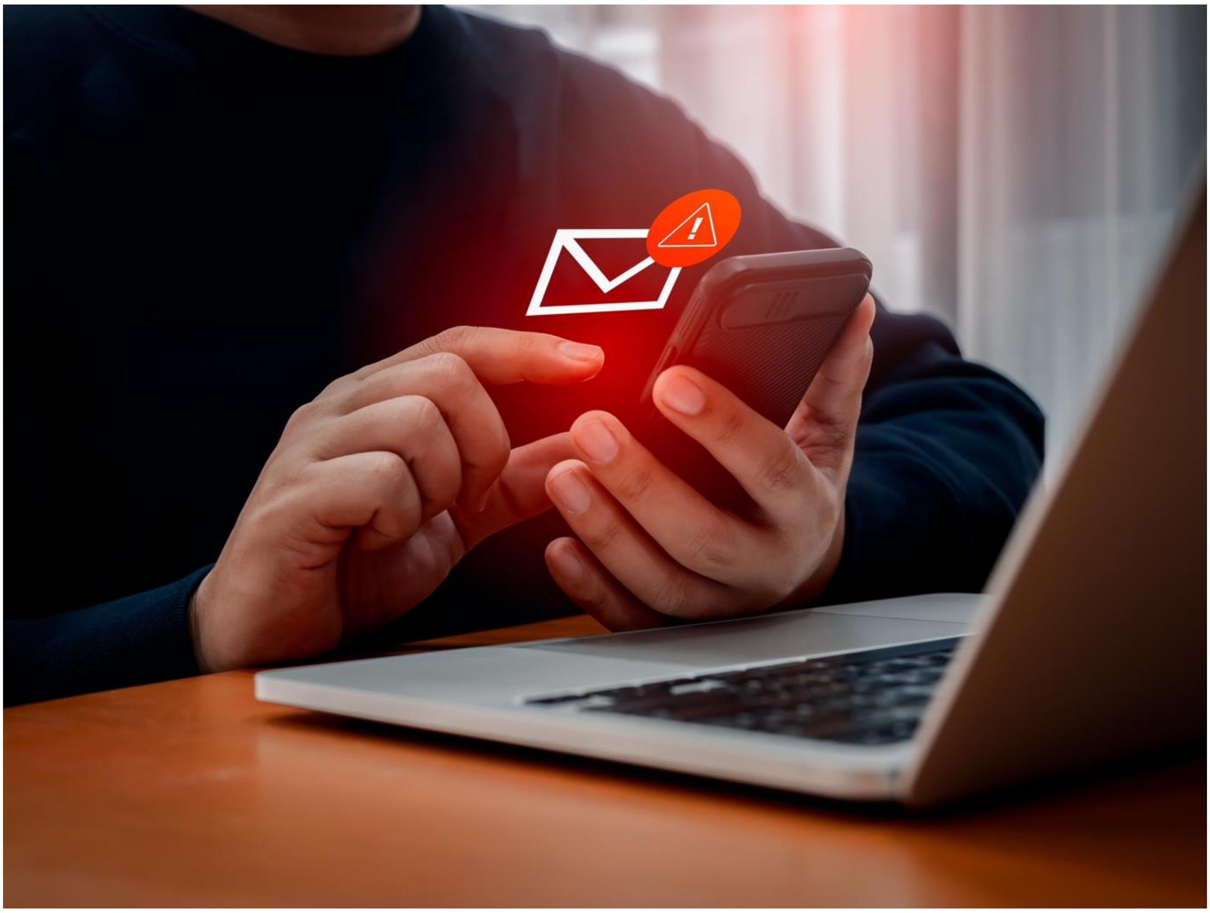

Image credit: Shutterstock

Online cloud experts from TelephoneSystems.Cloud have shared the signs that could mean you are the victim of a cybersecurity attack.

As more people engage in online activities like shopping, information sharing and online banking, criminals are able to target victims through more sophisticated scams, using AI software to make them look more legitimate.

This means it is easier than ever to gain access to an individual's information. But, looking for signs like unusually slow internet speeds, unexplained financial transactions and suspicious emails can help to detect security issues.

As well as providing insights into detecting suspicious activity, the online experts are also calling for Brits to take preventative measures to ensure their safety online.

Juliet Moran from TelephoneSystems.Cloud says: “Although many of us don’t like to think we would ever fall victim to an online scam or be part of a security hack - the truth is it really could happen to anyone.

“With so many more people creating online profiles, setting up banking apps or making big purchases through online stores, the opportunities for criminals are endless.

“Thats why we wanted to share some of the tell-tale signs your internet security may have already been compromised - and ways to prevent future security breaches.

“Many businesses have measures in place to protect their online security - and individuals should be doing the same.

“There are some really straightforward prevention methods - such as two factor authentication. This can help keep hackers out and protect personal details. There are also antimalware programs which monitor program behaviours. They can catch previously unrecognized malware and detect any suspicious activity.

“To prevent unauthorized payments from your bank, turn on transaction alerts and keep an eye on your bank statements to ensure there have been no strange payments out from your account.

“You can get in contact with your bank provider and request that they send you alerts before changing any of your notification options - so that a hacker isn’t able to turn off transaction alerts without you realising.

“As well as learning how to protect yourself - make sure to look out for family members and friends, particularly if they are vulnerable or elderly.”

Here are some of the signs your internet may be compromised, from TelephoneSystems.Cloud:

1. Frequently slow internet speeds

Slow internet speeds aren't uncommon and can be caused by a range of factors, such as Wi-Fi interference and the distance your connection is from your internet exchange. But slow and unstable internet speeds can also be the result of malware or viruses using your bandwidth for malicious purposes such as botnets or data infiltration.

2. You are seeing random popups

If you have noticed a sudden influx of random, frequent popups, it may be a sign your internet security has been compromised. In order to put a stop to these, you will need to get rid of any malicious-looking toolbars and programmes which may be installed on your device.

3. Unexplained financial transactions

Unexplained financial discrepancies can indicate a breach and may well be the result of email compromise or financial malware. Ensure that bank account changes are authorised by human interaction and not just an email.

4. Your online password stops working

If you have several unsuccessful attempts at logging in to online accounts with your correct password, it means a hacker has gained access to your account and changed the password to keep you out. This may be because you replied to a phishing email requesting information. If this happens, act quickly and contact the online service to report your compromised account and seek their advice and help for next actions.

5. Suspicious emails

A sudden increase in targeted phishing emails could indicate that an attacker is trying to compromise your accounts. These attempts are now using AI to look more convincing than ever. If you notice an increase in these types of emails it would be worth looking into strengthening your email security, spam filtering can assist with reducing these risks.

ENDS

Notes to editor: https://www.ncsc.gov.uk/guidance/data-breaches#section_2