



POLICE
SCOTLAND
POILEAS ALBA

Phishing, Smishing and Vishing

Police Scotland

Cybercrime Harm Prevention

04.03.25



'Phishing' is when criminals use scam emails, text messages (smishing) or phone calls (vishing) to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

How do I know if I've been phished?

If you've received a suspicious message, it may be a phishing attempt. It is important not to click on any links in the message or enter any information.

What to do if...

- **I've shared my banking details**

Contact your bank immediately and let them know. If you use online banking, you can cancel your card(s) online.

- **I think my account has been hacked**

If you can't access one of your accounts or have noticed other unusual activity, refer to our [actions to take to recover a hacked account](#).

- **I think my device has been hacked**

If you have opened a suspicious link on your device, or followed instructions to install software, open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds. Refer to our actions to take to recover [an infected device](#).

- **I've given out my password**

If you use the same passwords on other accounts, you should change them immediately.

- **I've lost money**

Tell your bank and [report it as a crime to Action Fraud](#) (for England, Wales and Northern Ireland) or [Police Scotland](#) (for Scotland).

- **I've received the message on a work laptop or phone**

Contact your IT department and tell them what has happened.

If you haven't entered any personal information, downloaded any files, or installed software, it is unlikely you need to take further action. But you should stay alert to emails and notifications on your accounts to check for any suspicious activity.

If you have entered personal details, including passwords, or followed instructions to install software, there are other things you can do:

- **You've opened a link on your device or followed instructions to install**

software: Open your antivirus (AV) software if you have it and run a full scan. Allow your antivirus software to clean up any problems it finds. If you don't have an antivirus or need more information [view our actions to take to recover infected devices](#).

- **You've entered personal details or passwords:** You should change the passwords on any of your accounts where you use the same password. If you've entered banking or card details, contact your bank straight away, and if you use online banking, cancel the card(s) there.

Reporting

The National Cyber Security Centre (NCSC) is a UK government organisation that has the power to investigate and take down scam email addresses and websites.


Reporting a scam is free and only takes a minute. By reporting phishing attempts, you can:

- reduce the amount of scam communications you receive
- make yourself a harder target for scammers
- protect others from cybercrime online

As of October 2024 the number of reports received stands at more than:

 **36m** reported scams

Which has resulted in:

 **200k** scams being removed across 363,864 URLs

Forward suspicious emails to report@phishing.gov.uk, texts to 7726