

GUIDANCE

Phishing: Spot and report scam emails, texts, websites and calls

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

Pages

Phishing: Spot and report scam emails, texts, websites and calls
Report a scam email
Report a scam text
Report a scam phone call
Report a scam website
Report a scam advert
Phishing scams: If you've shared sensitive information
How to spot a scam email, text message or call

PUBLISHED

26 November 2021

REVIEWED

26 November 2021

VERSION

2.0

WRITTEN FOR

[Individuals & families](#)

Was this article helpful?

Yes

No

How to spot a scam email, text message or call

IN THIS GUIDANCE

1. [Recognising online scams](#)
2. [How to spot scam messages or calls](#)
3. [How to report suspicious communications](#)
4. [Make yourself a hard target](#)

Recognise the signs someone is trying to scam you, and learn how to check if a message you have received is genuine.

Recognising online scams

Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust.

It used to be easier to spot scams. They might contain bad spelling or grammar, come from an unusual email address, or feature imagery or design that feels 'off'. But scams are getting smarter and some even fool the experts.

Criminals are increasingly using QR codes within phishing emails to trick users into visiting scam websites. As we explain, [QR codes are usually safe to use in pubs and restaurants](#), but you should be wary of scanning QR codes within emails.

How to spot scam messages or calls

Scammers try to quickly gain your trust. They aim to pressure you into acting without thinking.

If a message or call makes you suspicious, stop, break the contact, and consider the language it uses. Scams often feature one or more of these tell-tale signs.

- **Authority**
Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency**
Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
- **Emotion**
Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity**
Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

➤ Current events

Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

How to check if a message is genuine

If you have any doubts about a message, contact the organisation directly. **Don't** use the numbers or address in the message – use the details from their official website.

Remember, your bank (or any other official source) will **never** ask you to supply personal information via email, or call and ask you to confirm your bank account details. If you suspect someone is not who they claim to be, hang up and contact the organisation directly. If you have paper statements or a credit card from the organisation, official contact details are often written on them.

How to report suspicious communications

If you have received a suspicious message or call, or visited a suspicious website you should report it.

- [Report a scam email](#)
- [Report as scam text message](#)
- [Report a scam website](#)
- [Report a scam phone call](#)
- [Report a scam advert](#)

Make yourself a hard target



Criminals use information about you that's available online (including on social media sites) to make their phishing messages more convincing.

You can reduce the likelihood of being phished by thinking about what personal information you (and others) post about you, and by [reviewing your privacy settings within your social media accounts](#).

← [Previous page](#)

[Phishing scams: If you've shared sensitive information](#)

Topics

Phishing

PUBLISHED

26 November 2021

REVIEWED

26 November 2021

VERSION

2.0


WRITTEN FOR

[Individuals & families](#)

Was this article helpful?

[Yes](#) [No](#)


Also see



NEWS

19 Jul 2024


[Statement on major IT outage](#)
Following [the global IT outage on Friday 19 July](#), [affected organisations should put in place...](#)



BLOG POST

20 May 2024

[Business email compromise: new guidance to protect your organisation](#)
[How to disrupt targeted phishing attacks aimed at senior executives or budget holders.](#)



GUIDANCE

[Business email compromise: defending your organisation](#)
[How to disrupt email phishing attacks that target senior executives or budget holders.](#)