LATEST SCAMS

National Insurance

Criminals are using your National Insurance number as a hook to get hold of sensitive data. The phone rings and an automated message warns that your N.I. number has been compromised. You are told that the only way to fix the problem is to get a new number and to press one on your keypad to be put through to someone who can help you. If you do this a helpful person demands a load of your details and states a new N.I. number will be sent in the post. This is a con artist who will sell your details to fraudsters and could lead to you losing your money. Stay safe by hanging up on automated calls.

NHS Covid 19 vaccine

Fraudsters are sending emails and texts that offer the COVID-19 vaccine.
You get an email or text that claims to be from the NHS.
It offers the chance to sign up for the vaccine and wants you to click on a link.
The link goes to a **fake** NHS page and wants you to give personal and banking details. The page may look real but it's a copy to try to scam you into giving your details.
Remember, the vaccine is free and the NHS will never ask for a payment or for your banking details.
If you get an email or text like this, **don't click on the link or reply**, just delete it.
You can forward a scam text free of charge to 7726.

Working from home

This targets people working remotely from home.
Fraudsters send an email that claims to be from your employer's IT support department.
They can copy a company's email address to make a message seem genuine.
The message says you need new VPN configuration details to be able to work from home. It wants you to click on a link to get these details.
The link goes to a **fake** Microsoft 365 login page. The page may look real but it's a copy to try to scam your personal or financial details.
If you get an email like this, don't click on the link or reply. **Just delete it.**

Bitcoin Social media

Targeting Social media users, especially younger people.
Fraudsters are using social media to offer Bitcoin deals.
They send a message that promises to double your money.
This message has been seen on Twitter, Snapchat and Instagram.
If you get a social media message about Bitcoin, **don't reply.**
Before you delete the message, you can report it to the social media platform.

Council Tax

Fraudsters send an email that claims to come from the Government Digital Service Team.
The message offers a Council Tax Reduction of nearly £400 for people on a low income or who get benefits.
It wants you to click a link to claim your refund.
This link will go to a **fake** page to trick you in to giving banking details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it.

Netflix

Fraudsters send an email to Netflix customers that claims to come from Netflix Support.
The message says your account will be cancelled if you don't update your personal details within 24 hours.
It wants you to click a link to update them.
This link will go to a **fake** Netflix page. The page may look real but it's a copy to try to scam you in to giving login, credit card and billing address details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it.

Coronavirus Grant
Fraudsters send an email that claims to come from a government agency, like HMRC.
The message says your grant has been approved. This is pretending to be a scheme to help self-employed people during lockdown.
It wants you to click on a link to fill in your information.
This link will go to a **fake** page to scam you in to giving your personal and banking details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it.

TV Licence
Fraudsters send an email that claims to come from TV Licensing.
The message says your direct debit has failed and you need to pay to avoid prosecution. It also offers you six months free TV licence.
There's a link to click to get this offer.
This link will go to a **fake** page to scam you in to giving your personal and banking details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it.

Coronavirus Tax refund
Fraudsters send an email that claims to come from HMRC.
The message says you can have a tax refund because of the coronavirus outbreak.
It wants you to click on a link to get this refund.
This link goes to a **fake** page to try to scam you in to giving your personal and banking details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it.

World Health Organisation
Fraudsters send an email that pretends to come from WHO.
The message has a document attached with advice to help stop the spread of coronavirus.
It wants you to download the document.
But it's a **fake** document to try to put a computer virus on your device.
If you get an email like this, **don't download the document.** Delete the email. Don't reply to it.

Facebook bait and switch
Fraudsters are using social media posts to send fake links to viral videos. These will appear as shared posts on popular places like Facebook. This is a bait and switch scam. The link goes to a fake site with a video. But a pop-up will ask you to update your video player with a download. The download will infect your device with a virus to steal personal and banking details. It will also send the fake post to your friends to try and scam them too.

- If you're not sure who a person is on social media, then don't connect with them. Some accounts are fake and just try to steal details.
- Don't click on any links or attachments unless you know they're safe.
- Make sure a site is safe before you give personal details.

Free supermarket vouchers
You might see a free voucher offer on Facebook from Supermarkets. It looks real and says it's for 'Today only'. But it's a scam. The link takes you to a fake website to fill in a survey. Then to get the voucher you have to click on another fake link and share your personal details. There are no vouchers. And your details could be used to try and defraud you at a later date.

- Make sure a site is safe before you give personal details.
- Ignore sites and emails that offer free things if you give your personal details.
- Tell friends and family about this scam, especially if they shop at those stores.
- Don't click on any links or attachments unless you know they're safe.

Paypal social media

You may see fake PayPal social media posts that ask you to enter a prize draw. These will appear as promoted or shared posts on popular places like Facebook. They will ask you to follow a link to log on. This is a scam. The link will lead to a fake site to try and steal your personal details.

- If you're not sure who a person is then don't connect with them. Some accounts are fake and just try to steal details.
- Don't click on any links or attachments unless you know they're safe.
- Make sure a site is safe before you give personal details.

Apple ID

You may get an email that looks like it comes from Apple. It will tell you that your card has been used to order something. The subject of the email could be either 'Receipt ID', 'Receipt Order' or 'Payment Statement'. This is a scam. The email is fake and will try to get you to follow a link or attachment to cancel the order. The scam will try to steal your personal and banking details.

- Don't open emails if you don't know who sent them.
- Check the sender's email address to make sure it's genuine.
- Don't click on any links or attachments unless you know they're safe.
- If you're not sure about an email, call the sender using a number from their site. Don't call the number in an email or pop-up.

British Gas

You could get an email that looks like it's from British Gas. It will say that your latest payment by direct debit didn't go through and your gas supply could be cut off. They want you to click on a link to check and update your payment details. This is a scam. The link is to a fake site to try and get your personal or payment details.

- Don't open emails if you don't know who sent them.
- Check the sender's email address to make sure it's genuine.
- Don't click on any links or attachments unless you know they're safe.
- If you're not sure about an email, call the sender using a number from their site. Don't call the number in an email or pop up.

Coronavirus

People are using the coronavirus outbreak as an opportunity to try new scams by email, call and text.

One email has a PDF document with up-to-date advice on the outbreak. **This is likely to be a scam**.

The document could contain a computer virus to infect your device. This will then try to steal your personal or payment details.

- Don't open emails if you don't know who sent them.
- Even if you know the sender, don't reply if an email looks odd.
- Look out for spelling mistakes and a messy layout.
- Don't click on any links or attachments unless you know they're safe.
- If you're not sure about an email, call the sender using a number from their site. Don't call the number in an email or pop up.

Coronavirus scams even use online marketplaces such as Facebook to sell goods like face masks and hand sanitisers that don't exist.

Before you buy anything online it's best to do some research and check buyer reviews to make sure a seller is genuine. And always pay by card - that way you protect your cash.

Fake DVLA texts

There's been an increase in DVLA scams online.

The most popular scam is by text message. It will tell you that you're owed a refund and ask you to click on a link. The link will take you to a page which asks for personal or account details.

This is likely to be a scam to try and steal your details.

- Be careful about opening texts that you didn't expect.
- Don't click on any links or attachments unless you're sure they are genuine.
- If you're unsure, call the DVLA. Use a number from their website, not one from a text.

Paypal email

Fraudsters are using emails that look like they come from PayPal. The most common message will tell you that there's a 'problem with your account'. It will include a link to follow to sort the problem out. This is a scam. The link will take you to a fake PayPal site to try and steal your personal or banking details, or to infect your device with a virus.

- Don't open emails if you don't know who sent them.
- Check the sender's email address to make sure it's genuine.
- Don't click on any links or attachments unless you know they're safe.
- If you're not sure about an email, call the sender using a number from their site. Don't call the number in an email or pop-up.

Royal Mail email

You could get an email or a text that looks like it's from Royal Mail. It will say that they couldn't deliver a parcel and will give a tracking number. They want you to click on a link to confirm the parcel or pay a fee. This is a scam. The link is to a fake site to try and get your personal or payment details.

- Don't open emails if you don't know who sent them.
- Check the sender's email address to make sure it's genuine.
- Don't click on any links or attachments unless you know they're safe.
- If you're not sure about an email, call the sender using a number from their site.
- Don't call the number in an email or pop up.

Google Calender

Fraudsters are sending fake emails that include a Google calendar invite. The subject of the event is in Russian and has a link to a video call. This is a scam. The link is there to try and steal your personal or banking details, or to infect your device. Your spam filter should pick this scam up. But to help protect yourself, you can follow these steps:

1. Open Google Calendar settings.
2. Go to Event Settings, find Automatically Add Invitations and select the option 'No, only show invitations to which I've responded.'
3. Also, under View Options, make sure that 'Show declined events' is unchecked, so scam events don't appear after they're declined.
    - Don't open emails if you don't know who sent them.
    - Check the sender's email address to make sure it's genuine.
    - Don't click on any links or attachments unless you know they're safe.
    - If you're not sure about an email, call the sender using a number from their site. Don't call the number in an email or pop-up.

Disney+

Disney+ customers.
Fraudsters send an email that claims there's been 'unusual activity' on your account.
The message says your account has been locked and you need to create a new password. It could also say
that there's been a problem with your card payment details.
They want you to click an 'update account now' button.
This button goes to a **fake** Disney+ page. The page may look real but it's a copy to try to scam your personal or financial details.
If you get an email like this, **don't click on the link.** Delete the email. Don't reply to it