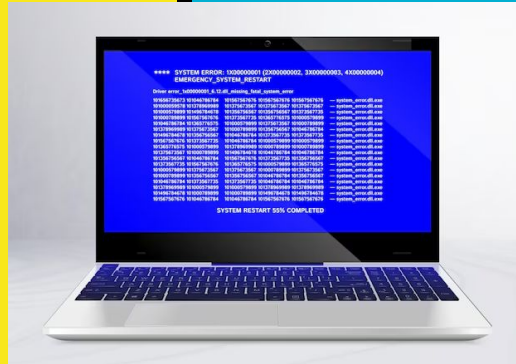


How to Identify and Avoid Scams



Smartphones - Scams

What we are going to cover:

- What are scams
- Common types of scams
- Whatsapp scams
- Scammers tricks
- Spot the warning signs
- How to protect yourself
- Useful information



Smartphone - Scams

What are scams?

A scam is a fraudulent or deceptive scheme to trick people, often to get money illegally.

Online scams are the **most common** type of fraud that aim to steal money or personal information through the internet but you can also be **targeted** by email, text/Whatsapp message or a phone call.

Scammers use tactics, like creating a **sense of urgency** or making **false threats**, to pressure you into acting quickly without thinking

Smartphone - Common Scams

Common types of scams:

- **Phishing:** a deceptive email that appears to be from a **legitimate source** to trick you into revealing personal information or sending money. These emails often contain **malicious links or attachments** that can steal your login credentials,
- **Government Impersonation:** Scammers pretend to be from a **government agency**, like the HMRC or DWP, to trick you into providing personal information or sending money *e.g. text with fake link that looks like UK Government website*
- **TV Licensing scam emails and texts:** Scam TV Licensing emails use subject lines like '**correct your licensing information**' or '**your bank declined the latest direct debit**'. They often try and convince you to hand over personal information such as bank details.
- **PayPal scam emails:** a scam email from PayPal about '**suspicious activity on your account**'. Other common scams tell you that your account has been suspended or that you are due a refund.

Smartphone - Common Scams

Common types of scams (cont):

- **Scam bank text messages:** Scam bank texts may ask you to **call a number** or **visit a website** to verify your details. A bogus text may also ask you for a pin or passcode, or tell you that you are due a refund. The message will try to alarm you and make you act quickly
- **Fraud recovery scams:** This is when fraudsters pretend to be a lawyer or a law enforcement officer/police and tell you they can help you recover the money you've already lost.
- **Mobile phone scams:** The National Fraud Intelligence Bureau (NFIB) are aware of an **ongoing scam** where consumers are being cold called by individuals impersonating employees of legitimate mobile network operators and suppliers. Victims are offered deals e.g.early handset upgrades and tricked into providing their online mobile account & bank account details

Smartphone - Common Scams (cont)

From: Netflix <rahma-cakupuyjya-vakangenlaaywa@bihvgh.com>

Date: September 14, 2020 at 6:05:32 AM GMT+2

To: [REDACTED]

Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.

Order Number : 38443246



Update current billing information

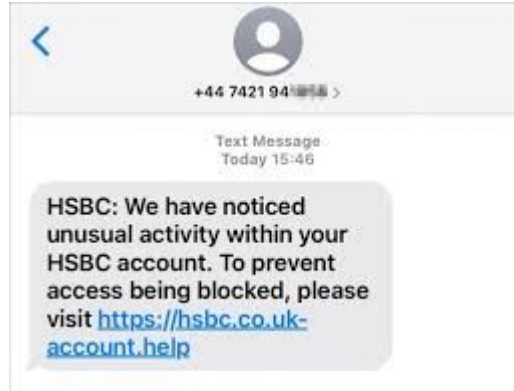
Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

TRY AGAIN PAYMENT

Obviously we'd love to have you back. If you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

- Netflix Team



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me



Dear PayPal customer,

Your PayPal account is limited. You have 24 hours to solve the problem or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?

We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[Confirm Your Information](#)

Smartphone - Common Scams (cont)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

REPORTING TYPES OF FRAUD PREVENTION

HOME > NEW WARNING AS CUSTOMERS TARGETED IN MOBILE PHONE SCAM

New warning as customers targeted in mobile phone scam

0 SHARES [f](#) [t](#) [in](#)

The National Fraud Intelligence Bureau (NFIB) are aware of an ongoing scam where consumers are being cold called by individuals impersonating employees of legitimate mobile network operators and suppliers.



Smartphone - Whatsapp Scams

Types of whatsapp scams:

- **Account takeover:** A scammer gets your Whatsapp account details and tries to log in with your phone number, which sends you a six-digit verification code. They will then message you from a different account, claiming they sent the code by accident and asking you to send it to them.
- **WhatsApp Gold:** This is a **fake** "upgrade" that promises exclusive features. The messages lead to a **malicious website** to download malware or steal data
- **Impersonation:** Scammers **pose as a trusted contact**, like a family member, by pretending to have a new phone number. They will create a sense of urgency and ask for money to help with an emergency

Smartphone - Whatsapp Scams (cont)

HOME > NEWSROOM > NEWS

Warning issued to WhatsApp users over account takeover scam

ALERT / 27-03-2023

0

SHARES



Most shared articles

Criminals are targeting WhatsApp users by posing as a friend and asking for a security code.



Scammers tricks

Here are **5 communication tricks** that scammers try to lure you in!

- **They create a sense of urgency**- *you are made to feel that is urgent and you have to act*
- **They encourage secrecy** - *use tactics like asking you to keep to yourself and stay on the phone so you feel that do not have time to confer with others*
- **They use a script** - *script is used as a persuasive tool, telling you what to do*
- **They use silence as a weapon** - *creates worry/doubt and start to create scenarios in your own head (psychological tactic)*
- **They boost credibility** - *you feel like the person is credible and there's no reason to suspect that it's a fraud, ask you to confirm personal facts/information*

Smartphone - Scams: Warning Signs

Spot the Warning signs!

- **Is it unexpected?** Scammers often call out of the blue. They may also try and contact you via email, text, post, social media, or even in person.
- **Do you feel pressured to act quickly?** Scammers might offer you a **bonus** or **discount** if you invest quickly, or they may say the opportunity is only available for a short time.
- **Does the offer sound too good to be true?** Fraudsters often promise tempting rewards, such as high returns on an investment.
- **Is the offer exclusively for you?** Scammers might claim that you've been specially chosen for an investment opportunity, and it should be kept a secret.
- **Are they trying to flatter you?** Scammers often try to build a friendship with you to put you at ease.
- **Are you feeling worried or excited?** Fraudsters may try to influence your emotions to get you to act.
- **Are they speaking with authority?** Scammers might claim that they're authorised and often appear knowledgeable about financial products

Smartphone - Scams: How to Protect Yourself

Do:

- **Treat all** unexpected calls, emails and text messages **with caution**. **Don't** assume they're **genuine**, even if the person knows some basic information about you.
- **Hang up** on calls and ignore messages **if you feel pressured to act quickly**. A genuine bank or business won't mind waiting if you want time to think.
- **Verify requests by calling**: If a bank, family member or friend makes an unusual request, call them on a trusted/official number to confirm it's them and not a scammer.
- **Use official websites** & look for '**https**' **at the beginning of the address and the padlock symbol**
- **Check your bank account** and credit card statements regularly for suspicious transactions.
- **Contact your bank ASAP** or their dedicated **spam service** if you are victim to a bank scam
- **Set up two-step verification**. This adds an **extra layer of security** and makes it harder for scammers to take over your account.
- **Sign-up to Verified by Visa or MasterCard Secure Code** whenever you are given the option while **shopping online**. This involves you **registering a password with your card company** and adds an additional layer of security to online transactions with signed-up retailers

Smartphone - Scams: How to Protect Yourself (cont)

Don't:

- **Click** on suspicious links: **Be wary of links** in emails or texts/Whatsapp from unknown contacts or those that seem too good to be true.
- **Give out** your bank account or credit card details unless you're certain who you're dealing with.
- **Share Whatsapp verification codes:** WhatsApp will never ask for your six-digit code.
- **Share your passwords** with anyone you don't trust (including your social media passwords).
- **Give access** to your device by **downloading software** or an **app** from a source you don't trust. (*Scammers may be able to take control of your device and access your bank account*).

Smartphone - Scams: Useful Information

BBC Scam Safe week: A special week of programming that started on Saturday 22 November highlighting what you can do to protect yourself and those you know from being scammed:

<https://www.bbc.co.uk/mediacentre/articles/scam-safe-week-everything-you-need-to-know>

Scam Interceptors: <https://www.bbc.co.uk/programmes/m00164f1>

Useful Websites or Phone Numbers

Action Fraud: Reporting and help with fraud/scams

<https://www.actionfraud.police.uk> or call 0300 123

Financial Conduct Authority: Help to protect yourself from scams

<https://www.fca.org.uk/consumers/protect-yourself-scams#section-common-financial-scam>

Smartphone - Scams

Remember

**Scams can be sophisticated, but if it sounds
too good to be true, it probably is!!**

Thank you

Any Questions?