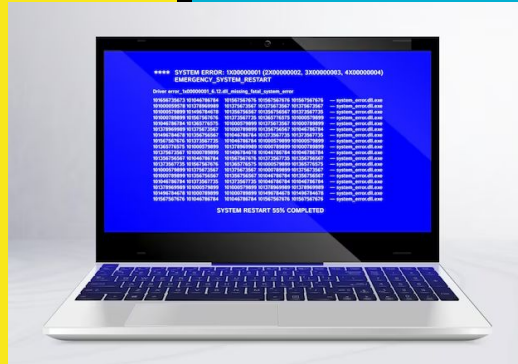


Scams



Smartphones - Scams

What we are going to cover:

- What are scams
- Common 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.

Phone or 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.

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 Phone Scams:

- **Banking scams:** Calls '*pretending to be your bank*' about *fraudulent use* of your *bank account or bank cards*. *Scammers* might ask you for your '**PIN**' and tell you to '*give your bank card to a courier*'. Your bank would never do this!
- **Undercover police scams:** Calls from someone *claiming* to be the '*undercover police*', saying that '*they're investigating a member of staff at your bank*' and asking for '**your card details**'. The police would never ask you to take part in an investigation like this!
- **HMRC scams:** A call from someone '*claiming to be from HMRC*' saying '*there's an issue with your tax refund or an unpaid tax bill*'. They may leave a message and ask you to call back. HMRC would never contact you this way and never ask you to reveal personal financial information!
- **Compensation calls:** A call '*from a company asking about a car accident*' you've supposedly had '*claiming you may be entitled to compensation*'. Don't engage in these calls! If you've had an accident, *call your own insurance company* on the phone number provided on your policy.

Smartphone - Common Scams

Common Online/Email Scams:

- **Fake websites:** Email 'claiming to be from trusted organisation e.g. your bank or HMRC' with a 'link to a fake website' asking you to provide your personal/financial details. A genuine organisation like your bank will never send you a 'link' asking you for your 'PIN, full password or financial details'
- **Email attachments:** Emails attachments you're not expecting. Some attachments contain 'viruses that infect your computer' if opened. These could seem to be from someone you know, but their account may have been hacked. Never click on email attachments that you're not expecting or look suspicious!
- **Fake tax refund emails:** Email claiming to be from HMRC, '***offering you a tax refund if you enter your details***'. HMRC would never email to give you a tax refund. This is a common scam and many people have had money stolen

Smartphone - Common Scams

Common Text Scams:

- **Fake Reward:** Fake text messages claiming to be e.g. from EE and Vodafone and promising prizes from their rewards schemes if click on the link. Do not click on any suspicious links/delete text
- **Fake bank text:** text claiming to be from your bank informing you that '***your account has been frozen and requests you call a new number***' Do not call the new number and delete text! Contact or visit bank if still have queries.
- **Fake package delivery:** official looking text claiming to be from delivery company/Royal Mail, attempted to deliver package but requires a small delivery fee e.g. £1.99. Click on link to make payment. Do not click on any suspicious links/delete text

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?

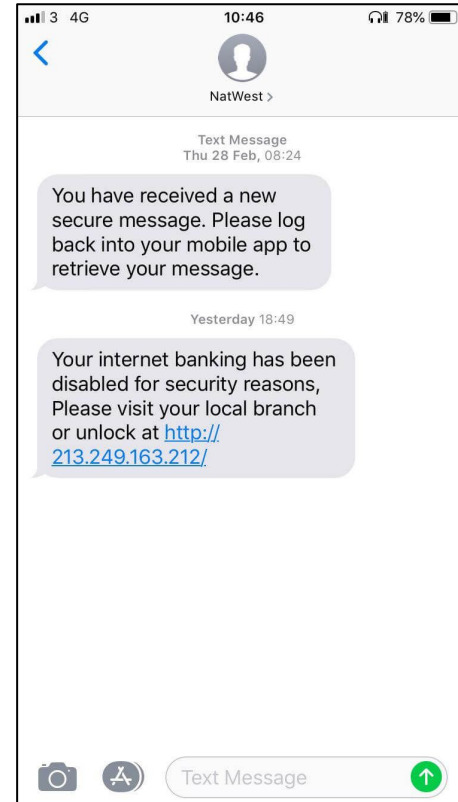
We believe that your account is in danger from unauthorized users.

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)



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!

1. **They create a sense of urgency**- *you are made to feel that is urgent and you have to act*
2. **They encourage secrecy** - *use tactics like asking you to keep it to yourself and stay on the phone so you feel that do not have time to confer with others*
3. **They use a script** - *script is used as a persuasive tool, telling you what to do*
4. **They use silence as a weapon** - *creates worry/doubt and start to create scenarios in your own head (psychological tactic)*
5. **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

What you should 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)

What not to do:

- **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

Useful Websites or Phone Numbers

Take Five: Scam Advice

<https://www.takefive-stopfraud.org.uk>

Age UK: Scams Advice

<https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud>

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

Stop and take a moment before parting with info or money!

Ask yourself could it be fake? Don't be afraid to challenge and say No!

Report scams to your bank *and* tell the Police:

reportfraud.police.uk

0300 123 2040

Scam Quiz

[BBC Scam Safe quiz: How scam savvy are you?](#)

Thank you

Any Questions?