citizens advice Wealden

SCAMS AWARENESS 2020

15TH JUNE 2020

TO

28TH JUNE 2020

'SPECIAL EDITION'

citizens advice Wealden

BEWARE

SOMEONE, SOMEWHERE WANTS YOUR MONEY AND IDENTITY

Council Tax Refunds

Early access Pension Fraud

Catfishing

Phishing

PPE

Charities

HMRC

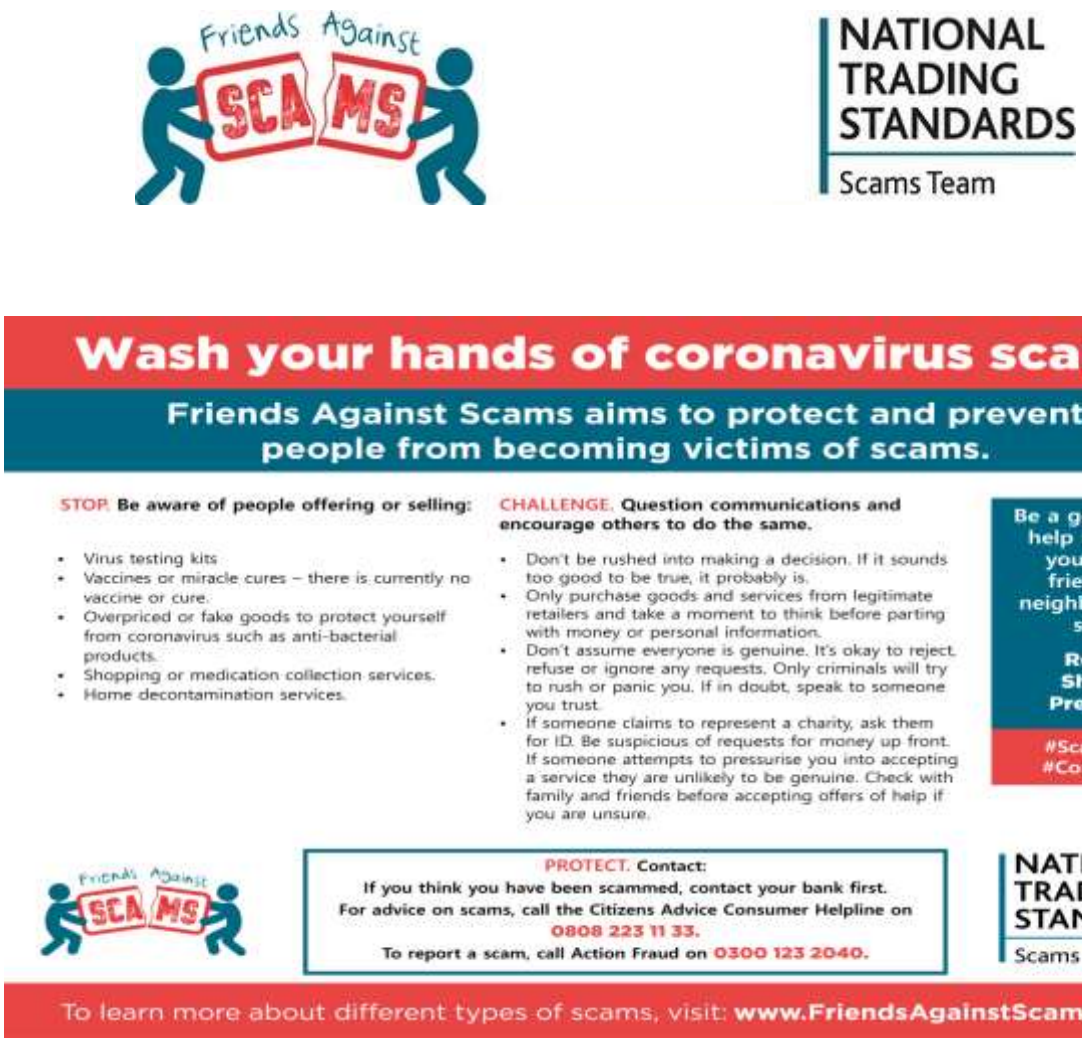
COVID-19 Fraud

Petfishing

Phone Calls

Text messages

Romance Scam



Friends Against Scams

Did you know that you can sign up to the Mailing Preference Service (MPS) to reduce the amount of direct marketing mail that you receive? Be aware that signing up to MPS will not stop all unwanted and scam mail reaching you.

Visit www.mpsonline.org.uk or call 0207 291 3310 #ScamAware

==========

ACTIONFRAUD

Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime.

What is fraud and cybercrime?

Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person. Cybercrime is any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet.

There are many words used to describe fraud: Scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick.
These are just a few words you might hear in relation to fraud. Fraud can be committed against individuals or businesses.

Facts about fraud and cyber crime

A 2019 Financial Cost of Fraud report estimates that the cost of fraud to the UK is anything between **£130bn - £190bn** a year with the Office for National Statistics (ONS) adding that people are more likely to fall victim to fraud or cyber offences above any other crime.

Between April 2018 and March 2019 there were:

- **741,123 crimes** were reported to Action Fraud.
- **£2.2bn** lost by victims.
- **65%** of reports were from businesses and **35%** from individuals.

==========

Which?

https://www.which.co.uk/

How to spot a scam

It can be difficult to spot a scam and fraudsters can be very cunning, but we have identified seven common signs of a scam.

Seven ways to spot a scam

It can be difficult to spot a scam. Fraudsters are extremely cunning and good at creating convincing scams.

You may avoid falling for scams by asking yourself these seven simple questions. If you answer yes to any of the following, there is a good chance it is a scam.

Fraudsters might seek to take advantage of uncertainty and confusion around Brexit to trick us into parting with our money.

Watch out for these Brexit scams which fraudsters may use before, during and after the UK's departure from the EU.

1. Contacted out of the blue?

An unsolicited call can be a sign of being contacted by a company you don't want to deal with.

However, companies do sometimes call their customers out of the blue for a legitimate reason.

If you're called by a company, make sure you do all you can to verify the identity of the caller.

Ask them to give you details that only the company will know e.g. your service contract details, payment details or bank account details.

If you're not 100% convinced of the identity of the caller, hang up and contact the company directly from a different phone.

There are some instances, though, where it's best if you're the person to instigate the first contact e.g. if you're looking to make an investment or if you're looking for a new bank account or credit card, you should always be the first one to make contact.

Scammers have increasingly been posing as the HMRC in calls, texts and emails.
If you're contacted out of the blue by someone claiming to be from the HMRC, perhaps saying you're owed a tax refund or there's a warrant for your arrest, it will almost certainly be a scam.

2. Is the deal too good to be true?

Scams will often promise high returns for very little financial commitment. They may even say that a deal is too good to miss.
Use your common sense, if a deal is too good to be true, it inevitably is.

3. Asked to share personal details?

Never share your personal details with anyone you can't validate is who they say they are.
Phone scammers will often try and get valuable personal data from you, and they can use this to steal your identity or steal your money.
Recent Which? research shows that 62% of people say they have been targeted by online fraudsters in the past 12 months.

4. Pressurised to respond quickly?

Never proceed unless you are absolutely certain your money will be safe. Once you transfer, it may be too late.
You should be especially weary if someone asks you to do a bank transfer as this offers the least amount of protection.
Scammers will often try to hurry your decision making, always take a breath and think things through.
Salesmen in particular should always give you time and space to make an informed decision anyone who tries to rush you is not to be trusted.

5. Are the contact details vague?

Vague contact details can be a PO Box Number, premium rate number (starting '09') or mobile number.
If anything goes wrong it's important you can contact those involved. This will be difficult if you don't have accurate contact information.

Premium rate numbers are also a favoured trick for squeezing every penny they can out of you.

6. Spelling or grammatical mistakes?

Legitimate organisations will rarely, if ever, make glaring spelling or grammatical mistakes, and if so they will usually be an isolated incident.

7. Are you asked to keep it quiet?

Being asked to keep something quiet should be a red flag. It's important you can discuss any agreements with your friends, family or independent advisors.

Often asking you to stay silent is used to keep you away from the advice and support you need in making a decision.

Emotional support after a scam

Being scammed can take a huge toll on your emotional wellbeing and mental health. It's often helpful to speak to someone about what you're going through.

This can be anything from a one-off scam to something which entangles you for months, every scam has an impact on your life no matter its size.

VS VICTIM SUPPORT

Victim Support has a free, 24/7 helpline where you can speak to someone confidentially.

This can be a one-off call or they can refer you to local services for on-going support.

This service is free and run by Victim Support which is an independent charity.

You can contact Victim Support by:

- Calling them for free on 0808 16 89 11
- Requesting online support

==========

Scams advice

https://www.bt.com/help/home/scams

Fraudsters are always coming up with new scams to gain access to your personal and financial details. By providing key advice and information, we want to help you protect your information and keep safe.

Fraudsters will use messages designed to look as if they are from a genuine company to try and trick you into giving out private information like your BT ID, username, password or bank details.

Fraudsters have used ransomware attacks such as, WannaCry and Petya as a hook to get people to click on links within BT branded emails.

Keep yourself safe – do not click on any links in a suspicious email. If you're unsure if an email appears to be from BT, rather than clicking on any links you should type www.bt.com/mybt in your browser to log into your My BT account.

What advice is BT giving to its customers to help them to protect themselves against scams?

We take the security of our customer's accounts very seriously and we are proactively warning our customers to be on their guard against scams. Fraudsters use various methods to 'glean' your personal or financial details with the ultimate aim of stealing from you.

- Our advice is that customers should never share their BT account number with anyone and should always shred bills. Be wary of calls or emails you're not expecting. Even if someone quotes your BT account number, you shouldn't trust them with your personal information.
- We will never ask customers for personal information out of the blue and we'll never call from an 'unknown' number.
- Where customers have fallen victim to this type of crime, we suggest signing-up for the CIFAS Protective Registration Service - https://www.cifas.org.uk/services/identity-protection/protective-registration

which in conjunction with more than 300 financial organisations aims to prevent further harm to individuals through on-going identity theft related crime, for example, for loan applications.

- We encourage anyone who's been scammed or the subject of an attempted scam to report it to Action Fraud – the UK's national fraud and internet crime reporting centre. This helps law enforcement agencies build up a wider picture that may help protect others.

==========

https://netflix.com/

I've received a suspicious email or text claiming to be from Netflix

If you received an email or text (SMS) requesting information like your username, password, or payment method that looks like it came from Netflix, it probably did not. Here are some tips to identify and handle a suspicious email or text and keep your account safe.

How do I know if an email or text is actually from Netflix?

Keep the following in mind to determine if it's from us:

- We will never ask for your personal information over email. This includes:
  - Credit card number
  - Bank account details
  - Netflix password
- We will never request payments via a 3rd party vendor or website.

What should I do if I received a suspicious email or text?

Scammers can't get any information from you unless you give it to them.

If you received a suspicious email

1. **Don't click** any of the links or open any of the attachments.
2. **Forward** the email to **phishing@netflix.com**.
3. **Delete** the email.

If you received a suspicious text message (SMS)

iPhone, iPad, iPod Touch

1. Tap and hold the message that you want to forward.
2. Tap **More...** and then the Forward arrow .
3. Enter **phishing@netflix.com.**
4. Tap Send .
5. **Delete** the message.

Android

1. Tap and hold the message that you want to forward.
2. Tap More and then **Forward.**
3. Enter **phishing@netflix.com.**
4. Tap Send .
5. **Delete** the message.

NOTE:

Text fees may apply.

What should I do if I opened a link or provided personal information?

- Change your Netflix password to a new, strong and unique one.
- Update your password on any websites where you use the same email and password combination.
- Contact your financial institution if you entered any payment information, as it may have been compromised.
- Forward the message to phishing@netflix.com with the steps above.

What are some best practices to keep my information safe?money

- Hover over any links before you click on them to make sure they lead where they are supposed to lead.
- Don't click the link when in doubt; go directly to the company website instead.
- Check the sender's address to see if it looks legitimate.
- Never provide personal or financially sensitive information through email.
- Install anti-virus software to help guard your devices and personal information.

Please contact us if you think someone has taken over your account so we can help you get back to streaming watching your favourite shows.

==========

https://www.actionfraud.police.uk/alert/how-to-protect-yourself-if-you-think-youve-been-affected-by-the-easyjet-cyber-breach

How to protect yourself if you think you've been affected by the EasyJet cyber breach

Action Fraud has been made aware by the National Cyber Security Centre of the cyber breach affecting EasyJet customers. We're currently monitoring our system for EasyJet related reports to see if there has been a significant increase.

At this time we're advising the public that if they think they've been a victim of fraud as a result of a data breach, to report it Action Fraud via the online reporting tool https://reporting.actionfraud.police.uk/login or by calling 0300 123 2040.

Here is what to do if you think you have been affected:

- **Phishing** – Criminals may use your personal details to target you with convincing emails, texts and calls. Be suspicious of unsolicited requests for your personal or financial details. If you receive an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): report@phishing.gov.uk

- **Financial details –** If your financial data was compromised, be vigilant against any unusual activity in your bank accounts or suspicious phone calls and emails asking for further information. If you notice any unauthorised transactions, notify your bank or card company.

- **Passwords –**Customers should ensure their passwords are secure. If you have been affected, you may want to consider changing passwords for key accounts such as banking.

  See Cyber Aware's advice https://www.ncsc.gov.uk/cyberaware/home on creating a good password that you can remember.

- **Report** - If you think you have been a victim of fraud or cybercrime, report it to us. https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

==========

citizens advice Wealden

https://www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/

Report a scam

(Advice applies to England)

If you've been scammed, there are organisations you should report the scam to.
Don't feel embarrassed about reporting a scam – scammers are clever and scams can happen to anyone.
Reporting a scam helps track down and stop scammers. This prevents other people from being scammed.

You should:

- protect yourself from further risks
- gather all the details of the scam
- report the scam to us
- report the scam to other organisations

Protect yourself from further risks

Coronavirus - be aware of new scams

It's important you're aware of the many new scams around at the moment because of coronavirus. Scams to look out for include:

-advertising face masks or medical equipment at high prices
-emails or texts pretending to be from the government
-emails offering life insurance against coronavirus
-people knocking at your door and asking for money for charity

If you see emails or texts about coronavirus from someone you don't know, or from an unusual email address, don't click on any links or buy anything.

Don't give money or personal details to anyone you don't know or trust - for example someone who knocks on the door and offers to help.

Before you report a scam, there are steps you can take to protect yourself from things getting worse.

When to call the police

Contact the police immediately by calling 101 if:

- the scammer is in your area
- you've transferred money to the scammer in the last 24 hours

If you feel threatened or unsafe call 999

Gather all the details of the scam

Write down the details of your scam. This will help you remember all the important information when you report it.

Make sure you include:

- who you've been in contact with – write down names, numbers and addresses if you have them
- why you're suspicious
- what information you've shared – for example, passwords, PINs, or bank details
- whether you've paid any money
- how you've paid – for example, credit card or bank transfer

Report the scam to us

How you report the scam to us depends on the type of scam it is.

Reporting an online scam

Online scams are scams that use the internet – for example, social media, emails and websites.

Report online scams through our Scams Action Service (Consumer Service)- https://ssl.datamotion.com/form.aspx?co=3438&frm=general&to=flare.fromforms

Reporting an offline scam

Offline scams are scams that don't use the internet – for example, doorstep or telephone scams.
Report offline scams through our consumer service- https://www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

What we'll do when you report a scam to us

Once we've got all the information we need, we'll pass this to Trading Standards. We don't investigate scams ourselves.
Trading Standards gathers information about scams so they can take legal action against scammers.

What Trading Standards does

Trading Standards will decide whether to investigate. They might contact you for more information.
Depending on what they find, they could prosecute the scammers or stop them operating.
Even if Trading Standards don't contact you, they might still use your evidence to take action in the future.

Report the scam to other organisations

You should also report scams to other organisations. This increases the chance of scammers being caught and stopped.
You should report all types of scams to Action Fraud, the UK's national reporting centre for fraud.
Action Fraud can get the National Fraud Intelligence Bureau to investigate scams. They'll also give you a crime reference number, which can be helpful if you need to tell your bank you've been scammed.

It's quickest to report a scam to Action Fraud online – https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime but you can also report the scam by phone.

Action Fraud

Telephone: 0300 123 2040
Textphone: 0300 123 2050
Monday to Friday, 8am to 8pm

Calls cost up to 40p a minute from mobiles and up to 10p a minute from landlines. It should be free if you have a contract that includes calls to landlines. Check with your supplier if you're not sure.

There are other organisations you should report your scam to, depending on what's happened.

If you got a scam email

Forward the email to report@phishing.gov.uk. It will go to the National Cyber Security Centre - they might be able to stop other people being scammed.

If you've been scammed through the post

Royal Mail investigates postal scams. If you've received something in the post you think is a scam, send it to 'Freepost Scam Mail'. Include the envelope it came in and a completed scam mail report. You can download a scam mail report from Royal Mail – https://personal.help.royalmail.com/app/answers/detail/a_id/303 or call them and ask for a form and pre-paid envelope.

Royal Mail
Email: scam.mail@royalmail.com
Telephone: 0800 011 3466
Calls are free from mobiles and landlines.

If the scam involves financial services

If the scam involves cryptocurrency, investments, insurance or pensions, report it to the Financial Conduct Authority - https://www.fca.org.uk/consumers/report-scam-us

If you think you've been scammed into transferring your pension, contact your pension provider immediately. Then get in touch with The Pensions Advisory Service - https://www.pensionsadvisoryservice.org.uk/contacting-us

If a scammer is imitating a company or person

Contact the real company or person to let them know their name is being falsely used.

A common imitation scam involves emails, texts or calls that seem to be from HM Revenue and Customs (HMRC). They might tell you about a tax rebate or ask for your personal information.

Report HMRC scams - https://www.gov.uk/report-suspicious-emails-websites-phishing/report-hmrc-phishing-emails-texts-and-phone-call-scams