More than £50 million lost to remote access tool scams last year

New data from Action Fraud, the national reporting centre for fraud and cybercrime, reveals that 20,144 people fell victim to scams where they were persuaded to grant criminals remote access to their device.

Victims reported losing a total of £57,790,384 – an average loss of £2,868 per victim.

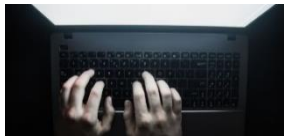
What are remote access tool scams?
Remote access tool scams will often begin with a browser pop-up saying that your computer is infected with a virus, or with a call from someone claiming to be from your bank saying that they need to connect to your computer in order to cancel a fraudulent transaction on your account.

Criminals will try to persuade the victim to download and connect via a remote access tool, which allows the criminal to gain access to the victim's computer or mobile phone. If the victim allows the criminal connection via the tool, they are able to steal money and access the victims banking information.

How to protect yourself

- Only install software or grant remote access to your computer if you're asked by someone you know and trust, such as a friend or family member, and never as a result of an unsolicited call, browser pop up, or text message.
- Remember, a bank or service provider will never contact you out of the blue requesting remote access to your device.
- If you believe your laptop, PC, tablet or phone has been infected with a virus or some other type of malware, follow the NCSC's guidance on recovering an infected device.
- Protect your money by contacting your bank immediately on a different device from the one the scammer contacted you on.
- Report it to Action Fraud on 0300 123 2040 or via police.uk. If you are in Scotland, please report to Police Scotland directly by calling 101.

Action Fraud also advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.



- **Stop**: Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge**: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect**: If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at police.uk or by calling 0300 123 2040.

Ticket to nowhere: don't let ticket fraudsters take off with your cash

Ticket fraudsters duped victims out of almost £4 million in the last year, as music and entertainment lovers bought tickets for festivals and events online as coronavirus restrictions eased.

New data from Action Fraud, the national reporting centre for fraud and cybercrime, reveals that 4,982 people fell victim to ticket fraud in the 2021/22 financial year.
Action Fraud received 623 reports of ticket fraud in September last year – the highest number of reports received since March 2020, as most festivals and events operated as usual for the first time since pre-pandemic.

Spot the signs of ticket fraud and protect yourself:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal give you a better chance of recovering your money if you become a victim of fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

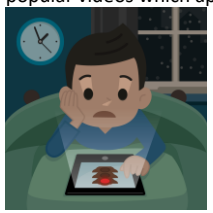
Huggy Wuggy: Parents and schools concerned about viral videos

The videos show a blue teddy-bear like character with sharp teeth, singing about hugging and killing.

Parents are being warned to be extra vigilant over seemingly fun videos that feature a menacing character with razor-sharp teeth.

The animated character goes by the friendly name of Huggy Wuggy, leading parents and children to believe the videos are aimed at youngsters and contain no inappropriate material.

But the blue bear-like creature chases and threatens other characters in nightmarish scenarios, leaving many children upset and frightened.
The character is from a survival horror game called Poppy Playtime but has been made into popular videos which appear on YouTube and have seemingly slipped through parental controls.



Poppy Playtime first appeared on Steam and is made by indie developer MOB Games. In it, the player plays as a former employee who is revisiting an abandoned toy factory previously owned by the game's in-universe company Playtime Co. 10 years after the staff have seemingly vanished without a trace.

The Huggy Wuggy character has also been recreated on Roblox, a virtual community where users can create their own 3D worlds with their own game players.

Primary schools concerned about Huggy Wuggy

West View Primary School in Hartlepool released a statement to parents on social media saying the character "sings worrying songs about hugging and killing".

It said: "In one of the videos, the bear asks the viewer to take their last breath. It is a very deceiving character, as hugs should be seen as something kind and love and because of its name is able to infiltrate firewalls and filters."

They have asked parents to be vigilant while their children are on YouTube.

Parents thought Huggy Wuggy was 'innocent'

Watch out for fake text messages pretending to be from the NHS. Since Jan 1st, 412 victims have reported losses totalling more than £531,000.

What you need to look out for:

- Be aware of requests for personal information in messages claiming to be from the NHS.
- Be alert to links or attachments in unexpected messages claiming to be from the NHS.
- Do not respond to requests for money, bank details or passwords. The NHS will NEVER ask for payment or any financial details.

How to report scam messages:

- If you are suspicious about an email, forward it to **report@phishing.gov.uk**.
- If you are suspicious about a text message, forward it to the number **7726** (it's free of charge).

MONTHS TOP TIPS:

MONTHS TOP TIP:

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook**:
www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**:
@SafeInWarks

Visit our **site**:
www.safeinwarwickshire.com

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.