December Cyber Scam Update

It could be you: Lottery fraud reports reach highest levels in two years

New data from Action Fraud, the national reporting centre for fraud and cyber crime, reveals almost £1 million has been lost to lottery fraud in the past seven months.

What is lottery fraud?

Criminals will contact unsuspecting victims informing them they have won a lottery or prize draw. The victim is then informed that they will need to pay an advance fee in order to receive their winnings. In reality, the winnings are non-existent and it is an attempt to steal the victims money, personal or financial information.

Between April and October 2021, Action Fraud received 629 reports of lottery fraud, with 89 per cent of reports mentioning well-known prize draws. Impersonation of People's Postcode Lottery accounted for almost half (49 per cent) of all reports.

Almost three quarters of victims (70 per cent) were aged over 50, with those aged over 65 accounting for 40 per cent of reports. Over half of the reports (59 per cent) mentioned being contacted via telephone. Other methods of contact reported by victims included email (21 per cent) and postal letter (10 per cent).

Almost have of victims (41 per cent) said they were asked to pay the advance fee to release the alleged winnings by purchasing gift cards and relaying codes to the fraudster.

Fraudsters use gift cards as a form of payment as they can be easily redeemed and sold on. These criminals also don't need the physical card to redeem the value and instead get victims to share the serial code on the back of the card with them.

In other instances, victims reported being asked for personal and financial information in order to obtain their alleged winnings. Some victims reported providing their bank details thinking they would be sent a small payment to verify the account. In reality, criminals will use these details to steal the victims money.

How to protect yourself

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

- **Stop:** Unsolicited offers of large sums of money in return for a small upfront payment should always raise a red flag. Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? Remember, you can't win a prize in a competition you didn't enter. 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 actionfraud.police.uk or by calling 0300 123 2040.

Public urged to donate safely this Christmas as it's revealed £1.6m was lost to online charity fraud over the past years.

The Fundraising Regulator, the Charity Commission for England and Wales, National Trading Standards and Action Fraud are joining forces to call on the public to give safely when donating online.
Data from Action Fraud reveals that £1.6m of the public's money was lost to online charity fraud over the past year.

The fraud captured by this data includes asks for donations for non-existent charities and the fraudulent collection of funds from genuine charities. Action Fraud's data shows that the £1.6m loss to fraud is up by 16% on the figure reported in the previous year.

The call for the public to give safely this Christmas is being co-ordinated by the Fundraising Regulator – the body which oversees charitable fundraising in the UK. It is encouraging the public to take steps to protect themselves online, particularly as the nation approaches the festive period, during which appeals for charitable donations increase.

The campaign is urging members of the public to conduct some simple checks before giving to charity, to make sure their donations reach the intended recipient. This includes:

- Check the charity name and its registration number on the Charity Commission website to find out whether the charity is legitimate.
- Use the Fundraising Regulator's online Directory to find out whether a charity has registered with it and committed to excellent fundraising.
- Look out for the Fundraising Badge on charity marketing materials – when people see it, they can have confidence in charity's fundraising.
- Ask questions about the cause – if people are still unsure about giving, they should always ask for more information. Legitimate causes will be happy to respond.

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.

December Cyber Scam Update

WhatsApp users urged to be wary over 'friend in need' scam

"If you receive a suspicious message... calling or requesting a voice note is the fastest and simplest way to check someone is who they say they are. A friend in need is a friend worth calling," said WhatsApp.

A new awareness campaign launched by WhatsApp and National Trading Standards says that 59% of people have either received a scam text in the last year or know someone who has.

The Stop. Think. Call. campaign aims to inform potential victims about the scams and educate them on how to protect themselves and their WhatsApp accounts.

Scammers can hijack WhatsApp accounts, often by using accounts they have already hijacked, to message friends and contacts asking for help.

Often these "friends in need" claim that they are sending their WhatsApp security code to the victim and ask for it to be sent back to them - however this security code belongs to the victim and enables the criminals to hijack their account.

Other scammers ask directly for money or personal information to be shared over the app.

THE NEW CAMPAIGN URGES PEOPLE TO:

- **STOP:** Take time before you respond. Make sure your WhatsApp two-step verification is switched on to protect your account, that you are happy with your privacy settings.
- **THINK:** Does this request make sense? Are they asking for money? Remember that scammers prey on people's kindness, trust and willingness to help.
- **CALL:** Verify that it really is your friend or family member by calling them directly, or asking them to share a voice note. Only when you are 100% sure the request is from someone you know and trust, should you consider it. If it turns out to be untrue, report it to Action Fraud.

MONTHS TOP TIPS:

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 real world.

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

Don't Clzone out when you part with your cash

Could you recognise a cloned company scam? Criminals are copying real websites to steal savings.

Could you recognise a cloned company scam?

The National Economic Crime Centre is targeting boomers in the run up to Christmas after latest figures from Action Fraud show more than £36 million has been lost to investment fraud via cloned company scams this year.

Data shows 34% of this age group were impacted by cloned company investment fraud in the first six months of this year, with average losses of £39,218 per victim.

Investment fraud by way of cloned websites has been on the rise in recent years, with Action Fraud reporting a total of £78 million lost last year – the year of the first coronavirus lockdown.

The crime is committed when fraudsters replicate or clone real company websites by using the name, address and 'Firm Reference Number' (FRN) attached to a company and authorised by the Financial Conduct Authority (FCA).

Once a fake website is up and running, fraudsters typically draw people in with adverts on search engine websites and social media.

The National Economic Crime Centre (NECC), part of the NCA, is working with City of London Police to reinforce steps that the public can take to protect themselves.

1. Reject unsolicited investment offers whether made online, on social media or over the phone. Be cautious when dealing with large sums of money, even if you initiated the first contact.
2. Always check the FCA Register to make sure you're dealing with an authorised firm and check the FCA Warning List of firms to avoid.
3. Only use the telephone number and email address on the FCA Register, not the contact details the firm gives you. Look out for subtle differences such as letters replaced with numbers (e.g. S and 5, O and 0), additional words, or spelling errors.
4. If you have visited a website you think is suspicious, report it to the National Cyber Security Centre, using their quick and easy reporting tool.
5. Consider seeking impartial advice before investing.

If you think you've fallen victim to an investment fraud, report it to Action Fraud as soon as possible online at http://www.actionfraud.police.uk or by calling 0300 123 2040.

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.