August Cyber Scam Update

Fraudsters targeting people with offers of 'free' or 'low cost' government grants and loans.

Victims have reported being offered the loans on their doorstep, via telephone, and over social media.

Fraudsters target victims who currently receive government benefits, or are eligible for Universal Credit:

- The victim is contacted by a fraudster offering them a 'free' or 'low cost' Government loan or grant.
- The fraudster requests personal and financial information from the target and uses these details to apply for Universal Credit in the victim's name, usually without informing the victim about it.
- The Department for Work & Pensions (DWP) approves the eligible claim and transfers money to the victim's account.
- The fraudster then requests that the victim transfer them a significant portion of the money as a 'finder's fee'.
- The victim receives a letter from DWP about their Universal Credit application and realises that they have been duped. The victim is then left to repay the total amount initially borrowed.

One victim was introduced to this scam by a friend on social media. The friend helped them receive the 'free grant' of over £1,000, only to later be asked to transfer £500 to the fraudster's account as a 'finder's fee'. The victim only realised they had fallen victim to a scam after they received a letter from DWP requesting repayments for the loan.

Protection advice:

- Never share your personal or financial information with someone you don't know and trust, especially if it's in response to an offer of "free money" or a "free grant".
- DWP will never approach you in the street or ask for your personal/financial details over social media.
- If you have concerns about your benefits, you should visit www.gov.uk/contact-jobcentre-plus
- If you suspect your identity may have been stolen, you can check your credit rating quickly and easily online. You should do this every few months anyway, using a reputable service provider and following up on any unexpected or suspicious results.

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.

Five stars or fake? How to beat fraudulent online reviews

Customer reviews have a huge influence over consumer spending, which is worth billions of pounds each year. When reviews are real, constructive and well-intentioned, they are of huge benefit to shoppers. Not so when they are fake.

A fake review will appear to have been written by a genuine customer but, unlike real reviews, they are paid for by the manufacturer or trader to boost ratings and rankings on sellers' websites – which in turn boosts sales. In some cases companies give away goods or refund purchases in return for glowing reviews. But these practices are illegal under consumer protection law.

But how can you tell if a review is fake?

- Be suspicious if a product has received a lot of five-star reviews in short space of time – on the same day for example. Be particularly wary if the product does not have a well-known brand. If the best-reviewed products are new or unheard of brands, and the top brands are ranked lower, be sceptical.
- Don't just look at the star ratings of a product: read the reviews. Do they sound natural or are they short and repetitive, using a lot of the same phrases? If so, beware.
- Where possible, filter your search for verified reviews (this means the reviewer bought the item or service). But remember to also treat this with caution – sometimes a consumer may have been refunded for a product they bought in return for a positive review.
- Look at the reviewer's history – have they given everything a five-star rating? What else did they buy? If they have bought 20 sets of similar headphones in the past week, for example, this should ring alarm bells.
- For hotel reviews, be wary of those that list the local amenities or attractions. Genuine hotel guests tend to focus on the room – space and cleanliness, for example, and hotel food: not what activities families can do nearby.

August Cyber Scam Update

Counterfeit currency: What to do if you receive counterfeit notes or coins and where to report

Only a small fraction of banknotes are counterfeit, but it is essential that they are reported to the police.

Last month, reports surfaced of criminals using social media platforms such as Instagram to promote and sell counterfeit money with sellers offering counterfeit notes for as little as a tenth of their face value.

In West Yorkshire, police confirmed a spate of incidents across the county in which counterfeit notes were used to pay for goods purchased online.

Victims made arrangements for the buyer to visit their home and pay in cash, only to find out afterwards that counterfeit notes had been used to pay for the goods.

In many cases, people are unsure about where to report counterfeit currency and what to do if they recover or are passed forged notes.

What to do if you receive counterfeit currency:

- If the notes have been passed and the suspect is not present, this should be reported via 101, by attending your local police station or online depending on the force area.
- If the suspect is present at the location or still nearby, consideration should be given to contacting the police on 999.
- Counterfeit notes should be retained and provided to the police as evidence, ideally inside a plastic wallet or paper envelope to preserve potential fingerprints.
- If there is CCTV footage of the suspect available, this should be downloaded and provided to the police together with the counterfeit notes or coins.

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.

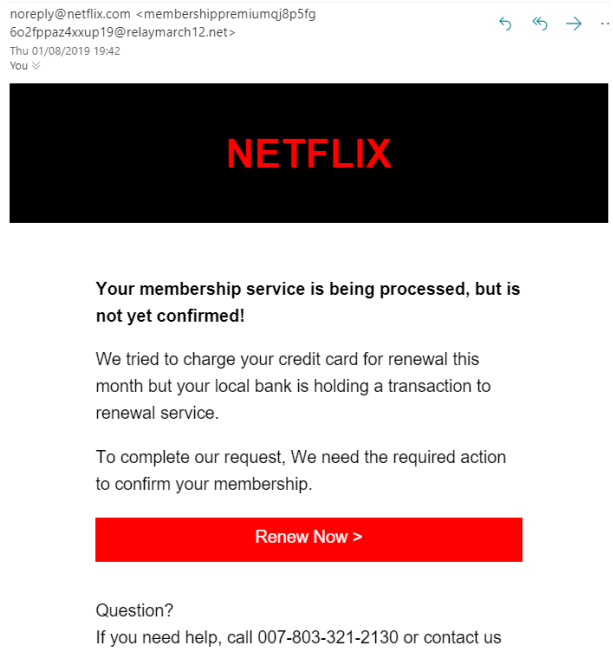
Like us on **Facebook**: www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**: @SafeInWarks

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

Suspicious Netflix phishing scams making the rounds

Some customers have been receiving fraudulent emails that look as if they were sent by Netflix, with the messages designed to trick the recipients into clicking a malicious link and handing over their login details and payment information.



Top Tips:

- Never enter your login or financial details after following a link in an email or text message. If you're unsure if you're visiting our legitimate Netflix website, type www.netflix.com directly into your web browser.
- Never click on any links or open any attachments in an email or text message you received unexpectedly, regardless of the source.
- If you suspect an email or text message is not from Netflix, do not reply to it.
- Instead, Netflix says you should forward the message to phishing@netflix.com, and then delete the email.

If You Are Affected

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.