September Cyber Scam Update

Over £44,000 lost to a PayPal scam that uses hacked Facebook accounts to lure victims

Action Fraud have received a surge of reports where victims have received messages through Facebook Messenger from friends and family requesting to use their Pay Pal account to receive funds from the sale of items on eBay. Overall, between 1st June 2020 and 31st July 2020 a total of 95 reports have been made with total losses amounting to £44,035.

Messages are sent by fraudsters purporting to be friends and family stating that they have sold a camera on eBay but that they are unable to process the payment as they either do not have a Pay Pal account or because their Pay Pal account is not working. The request is that the message recipient receives the funds into their own Pay Pal account, then, after transferring it into their own bank account, they forward it onto an account controlled by the fraudster.

If the victim agrees the payment is transferred into their Pay Pal account but, after the money is transferred out, the initial transaction is reversed leaving the account in negative balance. Multiple reports have also been received from victims stating that their Facebook Messenger accounts have been hacked and that these fraudulent messages have been sent to all their contacts on their behalf.

What you need to do

- **Verify financial requests:** Be wary of unusual messages asking for assistance with financial transactions. Even if the message appears to be from someone you know and trust, you should check it's really them that sent the message by calling them or speaking with them in person.
- **Unusual financial requests:** Never respond to any requests to send money, or have money transferred through your account, by someone you don't know and trust.
- **Secure your accounts:** You can protect your important online accounts by using a strong separate password and, where available, turn on two- factor authentication (2FA).
- **If you have made a payment:** Inform your bank, or payment service provider, such as PayPal, as soon as possible. They can help you prevent any further losses. You should also monitor your bank statements regularly for any unusual activity.

If you think you've been a victim of fraud, report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

164 Instagram users report losing over £350,000 to investment scams

During June 2020, Action Fraud received 164 reports from individuals falling victim to fraudulent investment schemes, commonly referred to as a 'money flipping' service offered by users on the Instagram social media platform.

Fraudsters approach (or are approached by) victims via the instant messaging feature of the platform after advertising their service. They claim to only require an initial investment of a few hundred pounds which they say will be used to trade on the stock market or to buy and trade foreign currency (Forex) until they have multiplied the investment several times within a matter of days which is paid to the victim after a small commission is deducted for the service.

In reality, once the initial investment has been transferred the victim is given a series of excuses as to why their money and 'profits' cannot be returned unless more money is sent. Eventually all contact is severed, and the victim is blocked by the suspect. Victims are usually requested to send the money by bank transfer or through a cryptocurrency platform which means it is nearly impossible to retrieve.

Spot the signs and protect yourself online

- **Unsolicited offers:** A common tactic used by criminals is to promote "investment" opportunities via social media accounts, promising large returns from a small up-front payment. Never respond to any requests to send money, or have money transferred through your account, by someone you don't know and trust.
- **Investment opportunities:** Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into making a transaction on the spot.
- **Seek advice first:** Speak with a trusted friend or family members and seek independent professional advice before making significant financial decisions.
- **FCA register:** Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money. For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

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

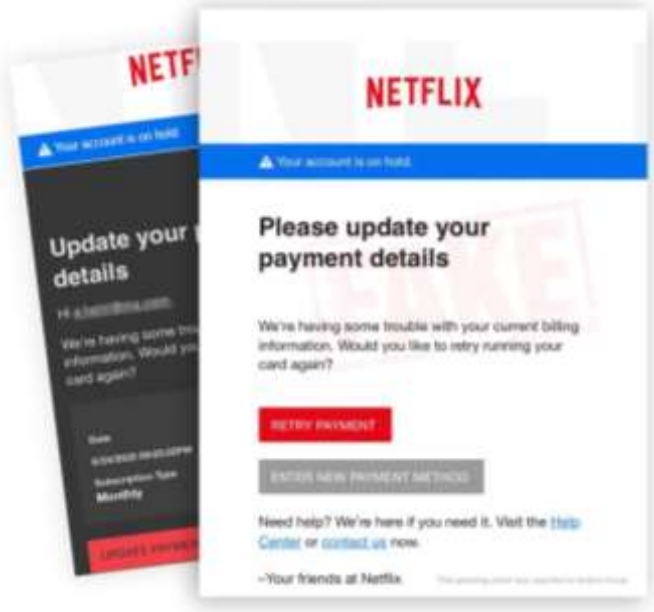
If you require support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

September Cyber Scam Update

Watch out for these fake Netflix emails

Action Fraud has received over 2,000 reports about fake emails purporting to be from Netflix. The emails state that the recipient's account is "on hold" due to payment issues.

The links provided in the emails lead to a genuine-looking phishing website that is designed to steal Netflix login details, as well as personal and financial information.



TOP TIPS:

- Your bank, or any other official organisation, won't ask you to share personal information over email or text. If you need to check that it's a genuine message, call them directly.
- Spotted a suspicious email? Forward it to the Suspicious Email Reporting Services (SERS) – report@phishing.gov.uk

MONTHS TOP TIP: Social Media

- Use a strong password. The longer it is, the more secure it will be!
- Use a different password for each of your social media accounts.
- Manage and regularly check your privacy settings.
- Never allow automatic logins. Don't have your computer's browser "remember" your login and password.
- Disable old accounts.
- Be selective when accepting friends, posting and clicking.
- Think twice before you post! Consider who will be seeing it.
- Avoid posting too much personal information.

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

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

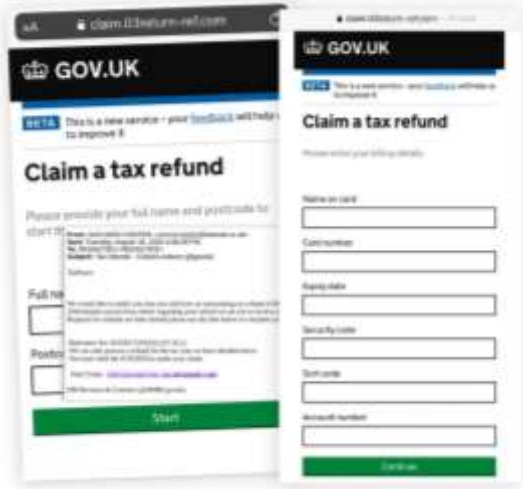
Follow us on **Twitter**: @SafeInWarks

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

Watch out for fake tax refund emails

Action Fraud received over 150 reports in 24 hours about fake emails purporting to be from the government departments, including HMRC. The emails state that the recipient has "an outstanding tax refund" that they need to claim urgently.

The links in the emails lead to genuine-looking phishing websites that are designed to steal persona and financial details.



TOP TIPS:

- Your bank, or any other official organisation, won't ask you to share personal information over email or text. If you need to check that it is a genuine message, call them directly.
- Forward suspicious emails claiming to be from HMRX to phishing@hmrc.gov.uk and texts to 60599.