February Cyber Scam Update

The Amazon Prime scam that has cost victims over £1M

Between 1 October 2019 and 16 January 2020, the National Fraud Intelligence Bureau (NFIB) identified 571 reports of Amazon Prime-related Computer Software Service Fraud. The scam has seen fraudsters steal over £1M from victims.

The scam, which we first reported on in October, involves victims receiving an automated call, informing them that they have been charged for an Amazon Prime subscription.

They are subsequently instructed to 'press 1' to cancel the transaction. When they do this, they are directed to a fraudster posing as an Amazon customer service representative. The fraudster advises the victim that their subscription was purchased fraudulently and that remote access to their computer is required in order to fix a security flaw that will prevent it from reoccurring.

The victim is asked to download a remote access application, often the 'Team Viewer' app, which grants the fraudster access to their computer.

The Team Viewer software is then mis-used by the criminal to monitor the victim logging onto their online bank account, which allows the fraudster to see the victim's personal and financial details. Other variants of the crime involve fraudsters stating that the recipient is eligible for a refund for an unauthorised transaction on their Amazon account.

Take steps to protect yourself:

Personal information
Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

Stay in control
Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's fine to stop the discussion if you do not feel in control of it.

Remote access
Never install any software or visit a website as a result of a cold call. Unsolicited requests for remote access to your computer should always raise a red flag.

Remember, if you have been a victim of fraud or cyber crime, report it to Action Fraud online or by calling 0300 123 2040.

TOP TIPS

- Avoid public Wi-Fi for any shopping, banking or entering of any personal information.
- Do not click on links in emails – go directly to the website the email is claiming to be from to verify any details or claim any offer.
- Look for https and either an unbroken padlock, key or the word Secure within the address bar when entering personal details online.
- Strong and unique passwords are key, try using three random words, mixed with CAPITALS, numb3r5 and punc+ua+!on to make your password more secure.

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 these fake emails from "your friends at Netflix"...

There has been an increase in the number of fake emails purporting to be from Netflix.

Have you received one of these emails asking you to update your Netflix account? Don't take the bait! The phishing emails state that the recipient must update their Netflix account information in order to resolve the issues.

The links in the emails lead to genuine-looking phishing websites that are designed to steal your Netflix password, personal and financial information.

TOPS TIPS:

- **Do not** click on links or attachments in suspicious emails
- **Never** respond to messages that ask for your personal or financial details.

February Cyber Scam Update

Fake PayPal emails lead to over £1 million in losses

Between October 2019 and December 2019, 3,059 crime reports were made to Action Fraud about fake PayPal emails. Victims reported losing a total of £1,121,446 during this time. Those targeted include people selling electronics, vehicles, phones and household furniture via online marketplaces

How the scam works
Fraudsters will send the victim an email purporting to be from PayPal in attempt to trick them into believing they have received payment for an item. The fraudster will then send a follow-up email requesting a tracking number in the hope that the victim will be rushed into shipping the item before they have had a chance to verify the payment.

What you need to do?

- **Sellers beware**: If you're selling items on an online marketplace, such as eBay, be aware of the warning signs that your buyer is a scammer. Don't be persuaded into sending anything until you can verify you've received the payment.
- **Scam messages**: Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.
- **Listen to your instincts**: If something feels wrong then it is usually right to question it.

PayPal offer the following advice:

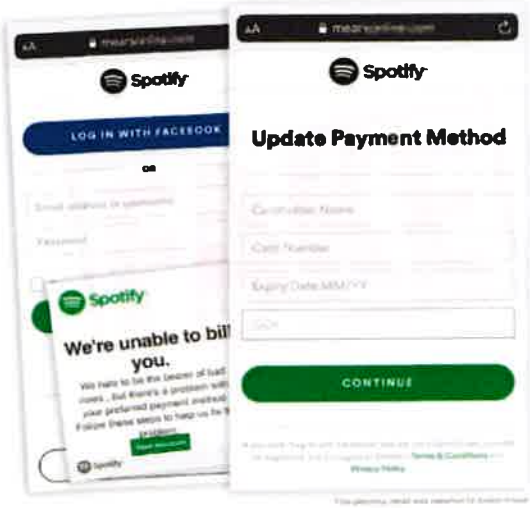
1. **Log into PayPal:** If you receive a suspicious email, don't act on the message or click on any links. Instead, open your browser, log into PayPal and check for any new activity. PayPal will also email or notify you in the app if you've received any payments.
2. **Check the basics:** Look out for misspellings and grammatical errors, which can be a tell-tale sign of a scam.
3. **Verify an email's authenticity:** Phishing scams will often mimic the look and feel of PayPal emails, and ask you for sensitive information – something that real PayPal emails will never do.
4. **How to spot the difference:** A PayPal email will address you by your first and last name, or your business name, and we will never ask you for your full password, bank account, or credit card details in a message.
5. **Avoid following links:** If you receive an email you think is suspicious, do not click on any links or download any attachments. You can check where a link is going before you click on it by hovering over it – does it look legitimate?
6. **Keep tabs on your information:** Limit the number of places where you store your payment information online by using a secure digital wallet like PayPal. If you are making a purchase online, consider using a protected payment method such as PayPal, so if your purchase doesn't arrive or match the product description, PayPal can reimburse you.
7. **Easiest of all, use common sense:** If a deal seems too good to be true, it probably is! Stay clear of exceptional deals or anything that is significantly reduced in price from what you would expect to pay.

If you think that you've received a phishing email, you can forward it to spoof@paypal.com, without changing the subject line. More information about our protection policies please visit our site: https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security

Fake Spotify scam emails on the rise!

Action Fraud have received over 40 reports in January about fake emails purporting to be from Spotify. The emails state that the recipient needs to update their account information in order to resolve payment issues.

The link in the emails lead to genuine-looking phishing websites that are designed to steal Spotify login credentials, as well as financial information.



TOPS TIPS:

- **Do not** click on links or attachments in suspicious emails
- **Never** respond to messages that ask for your personal or financial details.

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.