August Cyber Scam Update

PayPal account holders warned about phishing

The warning comes after Action Fraud received over 1,000 reports within 24 hours on 20 July 2020 about emails claiming to be from PayPal. The emails state the recipient's account has been "limited" as a result of a policy violation.

The emails then ask for customers to update their account or check the security of their account by clicking a link in the email. The links provided in the emails lead to genuine-looking websites that are actually phishing sites designed to steal PayPal login details, as well as personal and financial information.

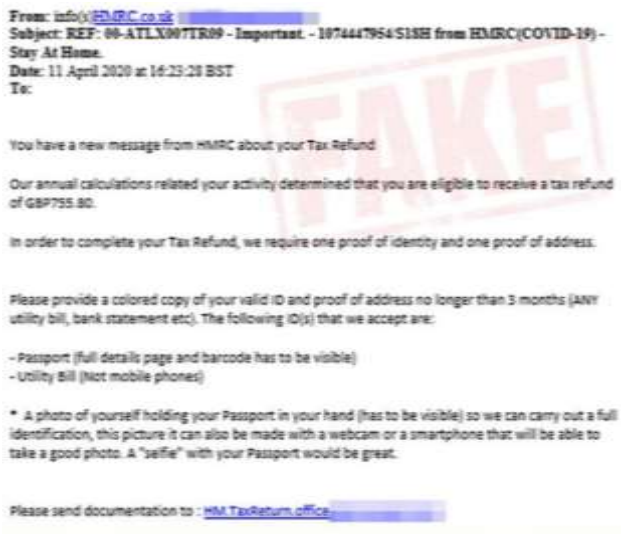
What to look out for and what you should do if you receive a phishing message:

- Official organisations, such as your bank, won't ask for personal or financial information by text or email. If you receive an email you're not quite sure about, you can report it by forwarding the email to the Suspicious Email Reporting Service at report@phishing.gov.uk.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm messages are genuine by using a known number or email address to contact organisations directly. You might find these on organisation's official website or from a letter you have received in the past.
- To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.
- A genuine PayPal email will only ever address you by your full name – anything that starts differently should immediately raise your suspicions. Look out for spelling mistakes, which are a common tell-tale sign of a fraudulent message. If you have any concerns regarding an email you have received, you should send it to spoof@paypal.com.

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.

Watch out for HMRC tax refund scams

Scammers are claiming to be from HMRC offering financial support as a result of Coronavirus.


From: info@HMRC.co.uk
Subject: REF: 00-ATLX007TR09 - Important. - 1074447954 518H from HMRC(COVID-19) - Stay At Home.
Date: 11 April 2020 at 16:23:28 BST
To:

FAKE

You have a new message from HMRC about your Tax Refund

Our annual calculations related your activity determined that you are eligible to receive a tax refund of GBP755.80.

In order to complete your Tax Refund, we require one proof of identity and one proof of address.

Please provide a colored copy of your valid ID and proof of address no longer than 3 months (ANY utility bill, bank statement etc). The following ID(s) that we accept are:

- Passport (full details page and barcode has to be visible)
- Utility Bill (Not mobile phones)

* A photo of yourself holding your Passport in your hand (has to be visible) so we can carry out a full identification, this picture it can also be made with a webcam or a smartphone that will be able to take a good photo. A "selfie" with your Passport would be great.

Please send documentation to : HM.TaxReturn.office

TOP TIPS:

- Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details, including requests to send images that prove your identity.
- HMRC will **never** text, email or phone you to ask for bank details, PINs or passwords.

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.

August Cyber Scam Update

Investment Fraud Alert: Friends & Family Unknowingly Recruiting Victims

Since June 1, 2020, Action Fraud has seen an increase in reports from people falling victim to Ponzi-style schemes that were advertised to them as “investment” opportunities.

A Ponzi scheme is a type of fraud where victims are lured in using the false promise of lucrative “investment” opportunities. In reality there is no investment and the money paid by victims goes straight into the pockets of criminals.

The fraudsters perpetrating the scheme will sometimes pay some of victims a little money as a way to convince them that the scheme is legitimate and to also incentivise them to recruit other victims. Most recently, the schemes have lured victims with investments including cryptocurrencies and foreign exchange trading (forex).

Fraudsters will often produce authentic-looking brochures and provide fictitious online trading accounts to investors in order to appear as though they’re a legitimate organisation. The reality is that will only keep in touch with victims via difficult to trace social media messaging platforms until the money stops being sent at which point, they will sever contact or demand payments to release the initial investment.

- **Seek Independent Professional Advice**: Before making significant financial decisions, speak with a trusted advisor who isn’t involved with the investment; this is equally important if you’re introduced to the scheme by someone you know. Just because you know someone who has also invested does not make the opportunity legitimate!
- **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.
- **Investment Opportunities**: Don’t be rushed into making an investment. Remember, legitimate organisations will never pressure you into making a transaction on the spot.
- **Investment Advice**: For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

THIS 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

Have you received an email from Netflix asking you to update your details? Don’t take the bait!

Action Fraud received over 1,400 reports last month regarding fake emails purporting to be from Netflix.

The fraudulent emails stat that the recipient’s account is “on hold” due to payment issues. The links provided in the emails lead to a genuine-looking phishing websites that are 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 Service (SERS) – report@phishing.gov.uk