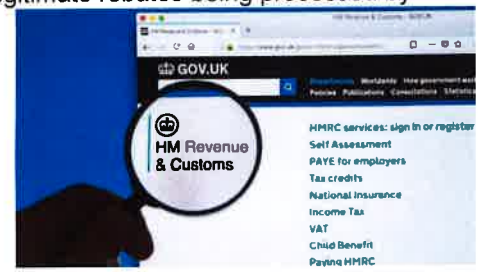
May Cyber Scam Update

Springtime tax scams target young and vulnerable, warns HMRC

Young adults who may have less experience of the tax system should be especially vigilant against springtime refund scams, warns HM Revenue and Customs (HMRC). Scammers are increasingly targeting vulnerable or elderly people and those with less familiarity with the tax system, such as young adults. During April and May, fraudsters regularly blitz taxpayers with refund scams by email or text pretending to be HMRC. Criminals do this to coincide with legitimate rebates being processed by HMRC.



They will encourage people to provide bank details, in exchange for a payment worth hundreds of pounds, on a fake government website to harvest private information and steal money. HMRC will never ask someone to provide bank details by text or email. Last Spring alone, HMRC received around 250,000 reports of tax scams — which is nearly 2,500 a day — and requested that over 6,000 phishing websites be deactivated.

When taxpayers file returns to HMRC, they will then legitimately receive a tax calculation as well as an email promoting them to check their Personal Tax Accounts. As many taxpayers file Self Assessment returns, most of HMRC's contact happens in the months after January. If you have paid too much tax, HMRC will issue the repayment automatically either direct into your bank account or if you have indicated on your tax return there is no bank account then HMRC will send you a cheque. If you have not paid enough tax, HMRC will tell you how much you owe and how you can pay securely.

Recognise the signs:

- Genuine organisations like banks and HMRC will never contact you out of the blue to ask for your PIN, password or bank details
- HMRC will **never** advise you of a refund in an e-mail or SMS message.
- Stay safe - don't give out private information, reply to text messages, download attachments or click on links in emails you weren't expecting.

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.

'£45 Tesco Voucher to Every Family' Facebook Scam

A post circulating rapidly on Facebook is claiming that large retailer Tesco is giving every family a free voucher valued at £45. The post features an image depicting one of the vouchers.

However, the post is fraudulent. It has no connection to Tesco and people who participate will never receive the promised voucher.

In reality, the post is just another Facebook giveaway scam designed to trick you into submitting your personal information on suspect websites. The information you provide on the sites will be shared with dodgy marketing companies who will inundate you with unwanted phone calls, emails, text messages, and letters.

This type of scam is very common on Facebook. The scammers who create this fraudulent giveaway post have used the names of many popular companies around the world.

May Cyber Scam Update

'AOL OATH Switch' Phishing Scam Email

According to this email, which purports to be from AOL, your account will be cancelled if you do not click a link to "switch to the new AOL OATH".

The message claims that the switch is necessary because AOL and Yahoo teamed up in 2017 to become one company called Oath. However, the message is not from AOL or Oath and the link opens a fraudulent website. It is a phishing scam designed to steal your AOL account login credentials.

It is true that Verizon formed a new subsidiary called "Oath" that incorporates both Yahoo and AOL. In this case, the scammers have capitalised on news of the merger to make their fake message seem more credible.

In April 2019, another version of the message began hitting inboxes. The new version falsely claims that your "AOL email address will stop working after 20th of APRIL 2019 unless you switch to AOL OATH". Again, the button in the email opens a fraudulent website designed to steal your account login details.

However, the email has no connection to Oath and it is not true that your account will be cancelled if you do not click the link. If you do click the link, a fake AOL login screen will load in your browser. The login screen asks for your username or email address as well as your account password, whereby scammers can collect your login information and use it to hijack your AOL account.

Top Tips:

- If you receive one of these emails, do not follow any links or open any attachments that it contains.
- It is always safest to login to all of your online accounts by entering the address into your browser's address bar or via a trusted app. If a company does require that you make changes to your account such as agreeing to an updated privacy policy, you will generally be informed of this via a message you see after you log in.

MONTHS TOP TIPS:

Ransomware is a form of malware that gives criminals the ability to lock a computer screen. The only way it says it can be unlocked is if you pay a ransom fee.

Avoid Ransomware getting onto your device by:
- not replying to, or clicking links in, unsolicited emails
- only visiting and downloading content from websites you know and trust (look for HTTPS, an unbroken padlock, or the word 'Secure' within the address bar)
- back up your files regularly to an external, physical hard drive

If you have ransomware on your computer:
- seek professional advice from an IT specialist, who may be able to remove malware from the device
- report it to Action Fraud (see details below)

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

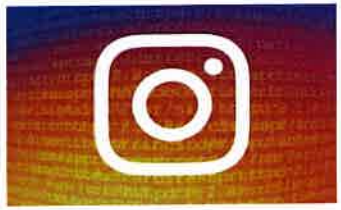
Visit our **site**: www.safeinwarwickshire.com

The Nasty List Phishing Scam is Sweeping Through Instagram

Targeting victim's login credentials, the hackers then utilize victim accounts to further promote the phishing scam.

The Nasty List scam is being spread through hacked accounts that send messages to their followers stating that they were spotted on a so-called "Nasty List". These messages state something like "OMG your actually on here, @TheNastyList_34, your number is 15! its really messed up." The scammers then attempt to send these messages to all followers of a hacked account.

If a recipient visits the listed profile, it will be named something like "The Nasty", "Nasty List", or "YOUR ON HERE!!". The profiles include a description similar to "People are really putting all of us on here, I'm already in 37th position, if your reading this you must be on it too." or "WOW you are really on here, ranked 100! this is horrible, CANT WAIT TO REVEAL THE TOP 10!"



These profile descriptions also include a link that supposedly allows you to see this Nasty List and why you are on it. For example, the above profiles are using the URL nastylist-instatop50[.]me, which when visited will display what appears to be very legitimate looking Instagram login page.

To avoid falling for an Instagram phishing scam like the Nasty List, if you are at a page that does not belong to the instagram.com web site, never enter your login credentials.

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.