January Cyber Scam Update

Mandate Fraud – notify your bank immediately if you see any unusual activity on your account

Mandate fraud is when someone gets you to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example a subscription or membership organisation or your business supplier.

How can Mandate fraud occur?

- You receive a letter in the post that appears to come from the company supplying a monthly magazine to you. It provides details of a new bank account and asks you to change the payment details to reflect this. The direct debit bank mandate is amended as instructed. The following month your magazine does not arrive and when you contact the publisher told that because your payment was cancelled you no longer have a subscription for the magazine.
- Your online bank account has been hacked into by a fraudster and monthly payment details are altered so that the money is transferred to the fraudsters account.
- you are contacted by someone pretending to be from an organisation you have a standing order with and request you change the order to reflect a change in their banking. The standing order mandate is changed accordingly but next month the actual organisation fails to deliver your products or a membership has been cancelled as they did not receive their payment.
- As a business you are contacted by someone pretending to be one of your suppliers and told they have changed their bank and could you amend the direct debit to reflect this. As a result the bank mandate is amended to the account that was provided. The next month you are contacted by your genuine supplier asking what has happened with the monthly payment.

Advice to avoid Mandate fraud

- Verify all invoices, as well as requests to change bank account details. To check that a request is legitimate, contact the supplier directly using established contact details you have on file.
- Access to sensitive financial information should be carefully controlled. Don't dispose of confidential documents without shredding them first.
- Check your bank statements regularly for any suspicious transactions. If you notice anything unusual, notify your bank immediately.
- For more information, please visit: https://www.scotland.police.uk/assets/pdf/keep_safe/bank-mandate-fraud

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.

Your chance to "win £500"... and also have your identity stolen!

Action Fraud have received more than 140 reports this week about fake Sainsbury's and Morrisons email. The emails state that the recipient has been "selected" to win £500 worth of supermarket vouchers.

The links in the emails lead to a phishing website that is designed to steal personal information.

TOP TIPS:

- Don't click on the links or attachments in suspicious emails
- Never respond to messages that ask for your personal or financial details.

January Cyber Scam Update

Beware of cash Isa scams

Fraudsters have been targeting savers by offering unrealistically high interest rates on cash Isas. The Bank of England's base rate is stuck at 0.75%, therefore when an advert for a cash individual savings account (Isa) paying "fixed returns of up to 9%", it can very appealing. However, this is a scam.

An investigation by The Times has found numerous websites advertising fake cash Isas from those promising seemingly impossible double-digit returns to others pledging investment opportunities in the 'alternative market'.

Many of the firms behind these Isas falsely claim they are regulated by the Financial Conduct Authority (FCA) or covered by the Financial Services Compensation Scheme (FSCS), which means up to £85,000 of your cash will be returned to you if the provider goes bust. The FCA has now put several of them on its fraud warning list.

How to spot fake cash Isas

- Be suspicious of all 'too good to be true' The best rate available on a genuine cash Isa is 2.01% for UBL UK's five-year bond. A cash Isa offering far more is likely to be a scam.
- The top rate for an instant-access Isa is 1.36% from Virgin Money, or 1.6% if you lock your money away for a year with Al Rayan Bank. To find real cash Isas stick to well-known comparison sites such as MoneyFacts, Moneysupermarket or Savings Champion. If you see a great deal, check the FCA's fraud warning list to see if they are aware it is a scam.
- And do some research to confirm a company has the professional backing it claims to have. You can check the FCA's register to see if a firm is authorised by them.

TOP TIPS: Set Your Cyber Resolutions

Set yourself cyber resolutions to stay safe while online.

New Year, New Passwords: make sure your passwords are strong. Try 3 random words with a number and some punctuation!

Update Your Software: take the New Year as a sign to refresh your device software so they are as secure as they can be.

Anti-Virus On Devices: many people do not have it across all the devices they use. You are only as secure as your weakest device - so make sure good practice is shared across all of them.

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

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

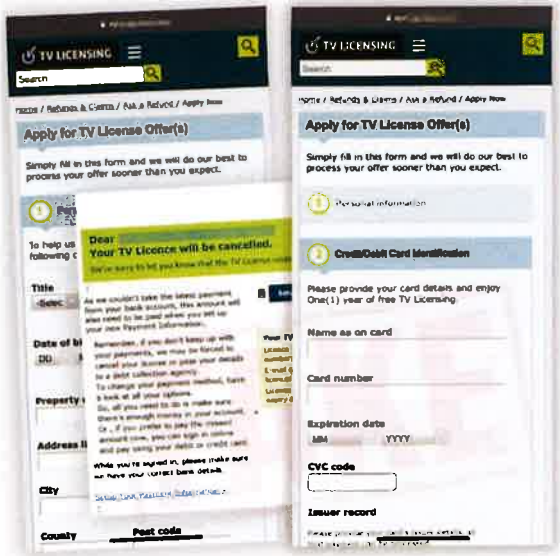
Follow us on **Twitter**: @SafeInWarks

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

Rise in fake TV Licensing emails

There have been over 2,500 fake TV licensing emails reported in recent months. The scam emails state that the recipient's TV licence will be "cancelled" if they do not provide their latest payment information.

The links to the emails lead to genuine-looking websites that are designed to steal personal and financial details. Don't take the bait!



TOP TIPS:

- Don't click on the links or attachments in suspicious emails
- Never respond to messages that ask for your personal or financial details.