SAFER

The Key to SAFER communities

Newsletter
April 2017

Email us on safer@wyjs.org.uk to sign up to this scam update.

SAFER Project and Safeguarding Real Stories

The SAFER team have collaborated with Bradford Council and Collingwood Learning to develop two monologues (Jean's story and Trevor's story) which talk through how they unwittingly became fraud victims and the impact it had on them.

http://realsafeguardingstories.com/index.php/jeans-story/
http://realsafeguardingstories.com/index.php/trevors-story/

If you would like the SAFER team to visit your community group to talk about doorstep crime and scams and fraud, please get in touch, our contact details are overleaf.

Solar Panel Scam

A new doorstep crime has been reported to Trading Standards. Fraudsters approach houses with solar panels claiming to be engineers working for the solar panel company. The fraudster tells the homeowner they are due a refund on their energy bill and have a chip and pin machine with them. The homeowner is asked to put their card and pin into the card machine and instead of a refund, money is debited from their account.

Stay safe by:-

- ✓ Verifying anyone who comes to your door claiming to work for the solar panel company by contacting the company yourself.
- ✓ Always use the number you have for the company and not a telephone number provided by the doorstep caller.
- ✓ Don't let anyone in who you don't know.

HMRC Tax Rebate Scams

There has been an increase in reports from people receiving unsolicited emails and texts purporting to be from HMRC claiming the recipient is due a tax rebate.

The texts and emails look genuine and ask the recipient to click the link to complete and submit a form in order to claim the refund. Victims are providing personal details which are subsequently used by fraudsters to impersonate victims who then find money has been taken from their accounts, new banking products taken out etc.

HMRC will never:-

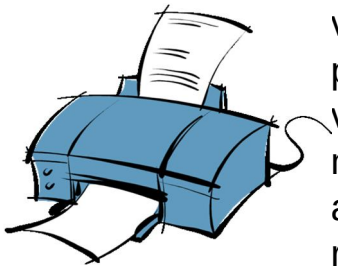
- ✓ Send emails or texts to tell you about a tax rebate or penalty payment. They will always send a letter.
- ✓ Ask for personal information or bank account details.

How to report

- ✓ Forward texts to 60599.
- ✓ Emails to: phishing@hmrc.gsi.gov.uk

Printer Helpline Scam

This scam works by fraudsters advertising a fake helpline number through online adverts, search engines, social media for example. The



victim contacts the fraudster requesting support with their printer issue. The fraudster then requests remote access to the victim's computer in order to fix the issue and then downloads malicious software (malware), accesses personal information and files or installs ransomware.

This is a clever fraud as the victim instigates the contact and unwittingly gives the fraudster access to their computer. There is no cold calling by the fraudster which makes the initial contact appear legitimate.

If you're having problems with your printer, here's how to stay safe:-

- ✓ Use the contact details provided by your printer manufacturer. These will be on the literature provided or on the official manufacturer's website.
- ✓ Do not use helpline numbers on adverts or posts on social media
- ✓ Make sure anti-virus software and online security is up to date which will reduce the risk of unwanted pop-ups advertising suspect services
- ✓ Be suspicious of any helpline that requests remote access to fix a printer problem. They should be able to talk you through the process.

Bogus Window Cleaners

Beware of anyone claiming to be collecting money on behalf of your regular window cleaner. Only pay your window cleaner or people you know work with your window cleaner.

Holiday Scams

With spring in the air, we're thinking about our next holiday and so are the fraudsters.

How does it work

The fraudster advertises 'bargain' holidays through fake websites which appear in internet search engines. The holiday is purchased and the money deposited straight into a fraudster's bank account. Most holidays are booked in advance and it can be months before a victim realises they've been scammed.

How to protect yourself:-

- ✓ Always make sure you use a trusted website.
- ✓ Don't book on websites that don't have a padlock icon (https) in the address bar.
- ✓ Be cautious if asked to pay by bank transfer using firms such as Western Union or MoneyWise which can be difficult to trace.
- ✓ Pay by credit card if you can.
- ✓ Make sure your holiday is ATOL protected.
- ✓ Get recommendations from family and friends.
- ✓ Report anything suspicious to Action Fraud on 0300 123 2040 or online.

LOTTERY FUNDED

West Yorkshire Trading Standards

THINK JESSICA

0113 393 9809
safer@wyjs.org.uk
www.facebook.com/SAFERProject
www.twitter.com/wytradstandards