# August Cyber Scam Update

## Argos Text Scams

Fake text messages have been reported to Action Fraud claiming to be from Argos. The fake text messages are claiming to offer a money refund for an overpayment that has been made. The link in the text message leads to a phishing website which will ask for personal information to verify details.

## WhatsApp Text Scam

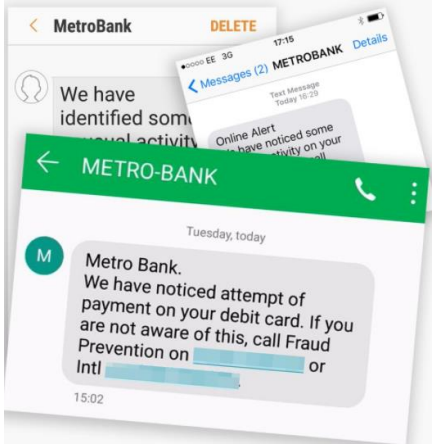
Messages pretending to be from Costa Coffee are circulating via WhatsApp and stealing personal data. Costa Coffee has confirmed it's a scam and its IT and legal team teams are in the process of issuing a take-down notice to the accounts. The scam states there are free vouchers being given away. There is a link in the email which leads to a fake website. Always consider if an offer sounds too good to be true and consider trying another way to find out.

## Amazon Email Scam

Fake emails claiming to be from Amazon are being sent by fraudsters. The subject line and the email differs however all of the emails that have been reported to Action Fraud have contained links to phishing websites that want you to sign in to a fake Amazon website.

## Metro Bank Text Messages

Fake Text messages are being sent out purporting to be from Metro Bank. The message will often say there is unusual activity on your account and you can call the fraud prevention team. Don't be tricked into giving a fraudster access to your personal or financial details. Do not reply to the messages or ring the number.




## TOP TIPS

- Never automatically click on a link or attachment in an unexpected email or text. Go through an app or the website.
- Phishing emails or texts that pose as a high-street name usually have poor spelling, grammar, graphic design or image quality. They may use odd 'spe11lings' or 'cApiTals' in the email subject to fool your email spam filter.
- Always go to your online accounts for high street stores to check on order history, personal details or vouchers you may be entitled to; rather than clicking on a link.

### 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.

# August Cyber Scam Update

## Password Sextortion Scam

Cyber criminals are sending victims their own passwords in an attempt to trick them into believing they have been filmed on their computer watching pornography and demanding payment. The emails contain the victim's own password in the subject line. It is thought the passwords may have been obtained from historic data breaches.

**TOP TIPS**

- Never be rushed or pressured into making a decision. Do not send any money.
- Secure it: Change your password immediately and reset it on any other accounts you've used the same one for. Always use a strong and separate password. Whenever possible, enable Two-Factor Authentication (2FA).

## Fake LinkedIn Emails

Fake LinkedIn emails are being sent on mass which claim your LinkedIn profile has appeared in multiple searches and the email provides a link for more details about the searches. The link leads to a malicious website which is designed to steal information.

**TOP TIPS**

- Never respond to emails you suspect might be fake, delete them or mark them as spam.
- Never follow Links, or open any attachments from emails you are not expecting.
- Always visit the correct website by searching for it in a web browser.

## Scam HMRC Phone Calls Warning By Trading Standards

The bogus callers attempt to frighten residents by falsely suggesting that the Police are on the verge of arresting them for unpaid taxes. The fraudsters then ask the residents to pay the bogus 'tax bill' often using iTunes gift card voucher codes. HMRC will never use texts to tell you about a tax rebate or penalty. End suspicious cold calls immediately.

### 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.

**MONTHS TOP TIP:**

**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.

**Follow Us on Social Media for the Latest Cyber Crime News**

Facebook facebook.com/cybersafewarwickshire

Twitter @CyberSafeWarks

Instagram Cyber_Safe_Warks

or visit www.cybersafewarwickshire.com