# May Cyber Scam Update

## Rise In So-Called 'Friendly Phishing' Emails


Action Fraud has received hundreds of reports from email users who have received a phishing email sent from a fraudster who describes themselves as a "law-abiding citizen".

The email claims the sender has accidentally received the email recipient's personal details. Attached to the email is a document which the fraudster claims contains the recipient's personal details.

The fraudster suggests that the email recipient's details may have been made available to scammers and they are contacting them to try to rectify the problem. To do so the recipient must open the document.

In reality, the attachment allows downloads malware onto the victim's computer. The malware attempts to obtain sensitive data from victims, such as banking credentials and passwords; this is subsequently used to take money from the victim.

In order to protect yourself from malware, having up-to-date virus protection is essential; however it will not always prevent you from becoming infected from strains of malware.

**TOP TIPS**

Don't click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication.

Always install device software updates as soon as they become available.

Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to is disconnected from your computer once any back-up is completed. This is because malware infections could spread to that device too, if connected.

If you think your bank details have been compromised, you should immediately contact your bank.

## NHS Scam Text Message

NHS England are warning about a bogus text message claiming to be from the NHS asking people to confirm both their year of birth and email address.

The NHS does **not** collect information this way.

If you receive this message, **delete it straight away**.

## Identity Theft On Facebook

Action Fraud are warning that fraudsters need just *three* pieces of personal information to steal your identity (full name; date of birth; and home address). Even more worrying is that most of these can be found on your Facebook profile.

30% of adults with a social media account include their full name and date of birth on their profile pages – making it easier than ever for criminals to commit identity fraud. Home addresses can easily be found if locations are attached to any posts.

**TOP TIPS**

- Update your privacy settings and ensure you are not revealing too much. Guidance on this can be found on the Safer Internet Centre website.
- Check to see if your location is attached to a status update before sending.
- Be aware of information posted about you as well! This could also include personal information.
- If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your full password, login details or account numbers.

**If You Are Affected**

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.

# May Cyber Scam Update

## Vodafone & O2 Scam Email Warning

VODAFONE and O2 customers have been told to look out for a number of scam emails which trick unsuspecting people into clicking dodgy links containing malware designed to steal bank details.


Customers who have received the emails are warned not to click on any links. The emails are littered with spelling and grammatical errors, which would never be in an official email.

If you receive these, or similar, emails, it is advised you delete them and do not click on any links contained.


## Supermarket Email Scams

An increasing number of residents have received emails claiming to be from supermarket chains.

One email claims to be 'Tesco', asking for a confirmation of payment for a recent online order. The email is received despite no online order being placed.

A second example claims to be from Sainsbury's' 'Inspired Rewards' service, whose system is being upgraded. The email then provides a link to customers who need to purchase any online shopping essentials quickly before the update begins.

Once you click on the links, the emails will ask you to pass over information, mainly your bank details.

In such cases, do not click on the links in the emails, and delete the messages from your inbox.

**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

## 245,000 UK Customers Affected By Wonga Leak

The payday loan firm Wonga has suffered a data breach which may have affected up to 245,000 customers in the UK.

Stolen information includes names, addresses, phone numbers, bank account details and sort codes. It may also include the last four digits of customers' bank cards – information used by some banks as part of the login process for online accounts.

**TOP TIPS**

Alert your bank and ask them to look out for any suspicious activity. Wonga will be informing financial institutions about the breach.

Watch out for scammers or unusual online activity. Customers are told to be cautious about cold calls and emails asking for personal information.

Change the password for your Wonga account and any other account with the same password.

## MAY'S TOP TIP: Book Your Holiday's Safely

Always use websites which have a green padlock and HTTPS within the address bar when paying for a holiday online.

Verify a company is genuine by checking their ABTA/ATOL numbers on the ABTA or ATOL websites.

When you are on holiday – DON'T post on social media that you are away (you might be letting potential burglars know your house is empty).

**If You Are Affected**

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or 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.

Make a scam/rogue trader complaint to Trading Standards via Citizens Advice Consumer Service on 03454 040506.