October Cyber Scam Update

Thomas Cook "refund" scams on the rise

Action Fraud have reported that on social media criminals are using the Thomas Cook liquidation as an opportunity to lure victims into financial scams. Members of the public have reported receiving calls and messages offering "refunds" by people purporting to be associated with, or acting on behalf of Thomas Cook.
We would urge people to be vigilant of unsolicited calls, texts or social media messages that ask for personal or financial details, and not to automatically click on the links in unexpected emails.

Legitimate organisations will never contact you out of the blue and ask for your PIN, card details, or full banking passwords. If you get a call or message asking for these, it's a scam. Remember, your bank or the police will never ask you to transfer money out of your account, or ask you to hand over cash for safe-keeping.

If you think you have been a victim of fraud, report it to Action Fraud on 0300 123 2040 or via our online reporting tool. For more information on how you can protect yourself, visit takefive-stopfraud.org.uk

Thomas Cook customers should go to https://abta.com/thomascook for details on how they can make a claim.

Here are our top tips for dealing with a suspicious call or message that arrived out of the blue:

- **Don't react immediately** – especially if the message is asking you to react urgently. Take five minutes to think carefully.
- **Get another opinion** – show it to a friend or family member. Does it look genuine to them?
- **Ignore any message asking for your bank details** – your bank will never ask you to share your bank details over text.
- **Don't follow any links in the text** – even if you think it's a genuine message from your bank, we recommend you don't follow any links or give any personal information to a text message you've received out of the blue.
- **Contact your bank separately** – contact your bank via their official website or official social media channel to ask if what you've received it genuine or not. Wait for at least five minutes to make a call to your bank if you received an unexpected phone call. And, ideally ring your bank from a different phone.

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.

One Billion Google Calendar Users Exposed to Fake Invite Scam

The flaw allows cyber criminals to take advantage of a default setting that automatically adds invitations to a person's Calendar when they are sent via email.

Unsolicited invites then appear as a notification through the Google Calendar app, which if clicked on can lead users to an official-looking page requesting personal and financial details.

Links within the event or notification will then take victims to a fake Google authentication page that captures their credentials.

Top Tips:

- Don't reply to event invites from your phone. Instead, follow the directions below to report the event as spam on your computer.
- When you report one event, all events from that organizer will be removed from your calendar.

How to report an event:

- On your computer, open Google Calendar.
- Double click the event you'd like to report.
- At the top, click More Actions Report as Spam.

If you don't want to see events on your calendar that you haven't replied to, you can change your Google Calendar settings:

- On your computer, open Google Calendar.
- At the top right, click Settings menu Settings.
- In the "General" tab, click Event settings, automatically add invitations.
- Select No, only show invitations to which I have responded.

October Cyber Scam Update

HMRC calls on universities to protect students from tax scams

New students starting university this year could be likely targets of a fresh wave of tax scams, HM Revenue & Customs (HMRC) warns. This comes as HMRC writes to UK universities advising them to warn new students about tax scams sent by fraudsters to steal students' money and personal details.

Fraudsters can use a range of methods to target students, most commonly by sending fake tax refunds using seemingly legitimate university email addresses (often ending in 'ac.uk') in order to avoid detection.

Depending on the details a criminal is able to obtain from a student, they could steal money, set up direct debits, make purchases for valuable goods on online sites or even take control of their computer – being able to access functions such as their webcam.

The letters to universities, authored by HMRC's Head of Cyber Security, encourages colleges to raise awareness of tax-related scams at the start of this academic year and to integrate scam advice into guidance for new students if not already established.

HMRC advised university leaders students are "more likely to be taken in" by tax scams because students may have "had little or no interaction with the tax system". This could make the offer of a tax refund from a scammer seem attractive, especially when on a budget.

Often HMRC-related email scams spoof the branding of GOV.UK and well-known organisations in an attempt to look authentic. The recipient's name and email address may be included several times within the email itself.

As well as email tricks, phone scams have also been used increasingly by criminals in an attempt to threaten taxpayers into handing over cash – HMRC had over 100,000 reports of such scams last year, compared to 400 in 2016. HMRC has since introduced defensive controls with Ofcom and mobile networks to curtail these scams.

If students receive an email offering money sent to them by someone claiming to be HMRC and it seems too good to be true, then they should report it to phishing@hmrc.gov.uk.

MONTHS TOP TIPS

- It's not just emails which criminals will use to scam people out of money, or to get their personal details.
- Text messages and social media are becoming increasingly popular methods used.
- Always double check before responding to a text -- Google the phone number used to see if others have reported issues with it.
- Just because it comes from a friend, doesn't mean it is always genuine – if it looks suspicious, don't click on the link, and don't reply with your personal details.
- Contact your mobile phone provider if you fall victim to a scam of this kind

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

2040 or http://www.actionfraud.police.uk

ime, contact Victim Support on 01926 682 693.

Want a free smartphone? The fraudsters are hoping you'll say yes!

Action Fraud has received over 60 reports purporting to be from PC World. The emails state there is a package, often a Samsung smartphone, waiting to be delivered to the recipient.

The link provided in the email leads to websites that are designed to steal personal information and financial details.

Top Tips:

- If it seems too good to be true, it is!
- Don't click on the links or attachments in *suspicious messages*
- Never respond to messages that ask for your personal or financial details.