June Cyber Scam Update

Fraudsters are continuing to send victims their own passwords in sextortion scam

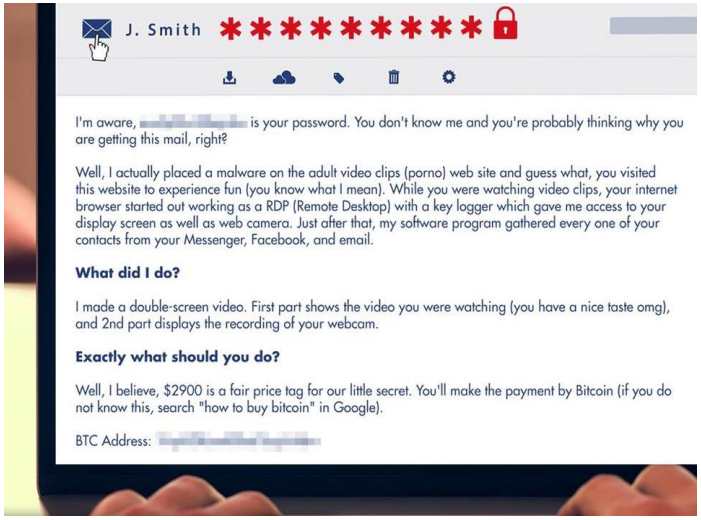
Fraudsters are sending victims their own passwords in an attempt to trick them into believing they have been filmed on their computer watching porn and demanding payment. In May alone, Action Fraud has received over 149 crime reports and 1,443 reports to our phishing reporting tool. Many victims reported receiving multiple emails over a short period of time. The emails contain the victim's own password in the subject line and demands payment in Bitcoin after claiming that the victim has been filmed on their computer watching porn.

Suspected data breach

Action Fraud suspects that the fraudsters may have gained victim's passwords from an old data breach. After running some of the victim's email addresses through 'Have I Been Pwned?' a website that allows people to check if their account has been compromised in a data breach, Action Fraud found that almost all of the accounts were at risk.

How to protect yourself:

- Don't reply to the email, or be pressured into paying: it only highlights that you're vulnerable and you could be targeted again. The police advise that you do not pay criminals. Try flagging the email as spam /junk if you receive it multiple times.
- Perform password resets as soon as possible on any accounts where you've used the password mentioned in the email. Always use a strong, separate password for important accounts, such as your email. Where available, enable Two-Factor Authentication (2FA).
- Always install the latest software & app updates. Install, or enable anti-virus software on your laptops & computers and keep it updated.
- If you have received one of these emails and paid the fine, report it to your local police force. If you have not paid, report the email as a phishing attempt to Action Fraud.



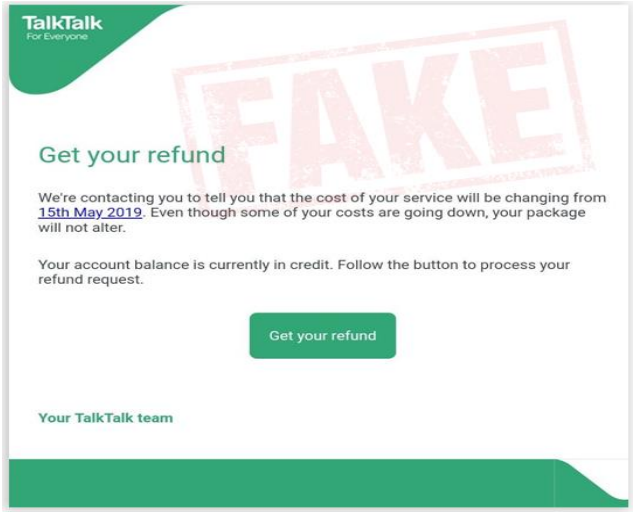
If You Are Affected

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.

Fake TalkTalk emails regarding refunds making the rounds

Action Fraud has received over 100 reports this week about fake emails purporting to be from TalkTalk. The emails state that the recipient's TalkTalk account is in credit and that they're owed a refund. The links in the emails lead to malicious websites.



Top Tips:

- Don't click on the links and/or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.
- It is always safest to login to all of your online accounts by entering the address into your browser's address bar or via a trusted app.
- Don't assume an email is authentic, even if someone knows your basic details (such as your name or address). Remember criminals can spoof email addresses to appear as companies you know and trust.

June Cyber Scam Update

Action Fraud report reveals £7 million lost to holiday fraud

Over 5,000 people reported to Action Fraud that they had lost a total of just over £7 million to holiday and travel related fraud, an increase on last year, when 4,382 victims reported losing £6.7 million. The average amount lost was £1,380 per person but, as in previous years, in addition to the financial cost, victims have also reported the significant emotional impact caused by this crime.

Over half, 53%, of the crimes reported were related to the sale of airline tickets. The next most common fraud at 25%, related to the sale of accommodation, with a peak in reported losses in October. This indicates that many victims report their loss after the end of the summer holidays the busiest time of the year for travel and a popular target for fraudsters.

Top Tips:

- Stay safe online: Check the web address is legitimate and has not been altered by slight changes to a domain name.
- Do your research: Don't just rely on one review - do a thorough online search to check the company's credentials.
- Look for the logo: Check whether the company is a member of a recognised trade body such as ABTA. If you have any doubts, you can verify membership at abta.com.
- Pay safe: Wherever possible, pay by credit card and be wary about paying directly into a private individual's bank account.
- Check paperwork: You should study receipts, invoices as well as terms and conditions. Be very wary of any companies that don't provide any at all. Use your instincts: If something sounds too good to be true, it probably is.
- Report it: Victims should contact Action Fraud via actionfraud.police.uk.

June Top Tips:

Book Your Holiday's safely!

When booking to go away this year, always remember the following:

- 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 criminals know your house is empty).

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

Coming this summer – seasonal **Social Media Update newsletter** for parents and carers!

REMINDER: WhatsApp urges users to act after confirming cyber surveillance attack

In mid-May cyber attackers were able to install spyware on WhatsApp through its voice call function, even if the user didn't pick up the call. Often, the call would disappear from the device's call log, so no visible trace was left.

Dozens of WhatsApp may have been targeted in the attack which exploited a major vulnerability in the app in an attempt to take over the operating system.

The breach was discovered in early May and has since been fixed. Users are urged to update their app to the latest version.

Top Tips:

- **Facebook is urging WhatsApp users to upgrade to the latest version of its messaging service.**
- Android: Go to Play Store, then tap Menu > My apps & games. Tap UPDATE next to WhatsApp Messenger
- iPhone: Go to App Store, then tap Updates. Tap UPDATE next to WhatsApp Messenger
- Windows Phone 8.1: Visit the store and select menu. Click on 'My apps' and select WhatsApp to update.
- Windows Phone 10: Visit the Microsoft store and click on 'Menu'. Select 'My Library' and tap 'Update' next to WhatsApp.