May Cyber Scam Update

Fraudsters send victims own passwords in sextortion scam

A sextortion phishing scam, first identified by the National Fraud Intelligence Bureau (NFIB) in July 2018, continues to be reported to Action Fraud in high numbers.

So far this month, Action Fraud has received 9,473 reports of this email scam, with 200 reports made in the last week.

The emails contain the victim's own password in the subject line and demand a payment in Bitcoin to prevent videos of the victim, on their computer visiting adult websites, being shared.

An example email reads;
"It Seems that, XXXXXX, is your password.
I require your complete attention for the upcoming 24 hrs, or I may make sure you that you live out of guilt for the rest of your lifetime.
Hey, you do not know me personally. However I know all the things concerning you. Your present fb contact list, mobile phone contacts along with all the digital activity in your computer from past 176 days.
Which includes, your self pleasure video footage, which brings me to the main motive why I'm composing this particular mail to you.
Well the last time you went to see the porn material websites, my malware ended up being activated inside your computer which ended up documenting a beautiful footage of your self pleasure play by activating your cam.
(you got a unquestionably weird taste by the way haha)
I have the full recording. If, perhaps you think I am playing around, simply reply proof and I will be forwarding the particular recording randomly to 8 people you know."

TOP TIPS

- Do not reply to the email or click on any links contained within it. Instead, report it to: report@phishing.gov.uk and then delete it.
- Do not be tempted to make the Bitcoin payment. Doing so may encourage the criminal to contact you again for more money.
- If you have made the Bitcoin payment, then report it to your local police force by calling 101.

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.

Victims of Coronavirus-related frauds have lost £2,759,579

Action Fraud have received 1,289 reports from victims of corona-virus-related frauds, with losses totalling over £2.7 million. The majority of these reports relate to online shopping scams where the victims purchase goods that were never delivered. They have also received 4,727 reports related to coronavirus-themed phishing emails.

TOP TIPS:

- Watch out for scam messages: Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.
- Shopping online: If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. Where possible, use a credit card to make the payment, as most credit card providers insure online purchases.
- Protect your devices from the latest threats: Always install the latest software and app updates to protect your devices from the latest threats.

May Cyber Scam Update

Criminals preying on financial worries as they spoof government websites to steal money

Criminals are continuing to exploit the COVID-19 pandemic to defraud innocent people, including sending fake emails and texts purporting to be from HMRC.

The emails stated that the recipient was eligible to receive a tax refund of up to £775.80. To complete the refund, recipients were asked to send proof of identity and proof of address. Documents that were suggested included a person's passport and a utility bill.

Action Fraud reported that the phishing emails were in the style of official 'GOV.UK' emails and using the same logo and branding. These emails told the recipient they could get a reduction in their council tax because they were on a low income or receiving benefits. A link was provided for recipients to claim for their reduction which, they are told, will be transferred directly to their bank account.

They have also received a number of other reports of phishing emails and texts purporting to be from government, including reports relating to universal credit, fines for leaving the house during lockdown and one-off payments of "COVID relief".

If you think you have been a victim of fraud, please report it to Action Fraud at https://www.actionfraud.police.uk or by calling 0300 123 2040. If you live in Scotland, please report directly to Police Scotland by calling 101.

MONTHS TOP TIPS:

Looking after your health and wellbeing

To help yourself stay well while you're at home:

- stay in touch with family and friends over the phone or on social media
- try to keep yourself busy – you could try activities like cooking, reading, online learning and watching films
- do light exercise at home, or outside once a day

#StayHomeSaveLives ☺

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

Watch out for these fake Tesco emails

Action Fraud have received 30 reports in the last month about fake emails that purport to be from Tesco.

The email states that the supermarket is offering free vouchers during the Coronavirus outbreak. The link in the email leads to a genuine-looking phishing website that is designed to steal login credentials as well as personal and financial details.

TOP TIPS:

- Do not click on the links or attachments in suspicious emails
- Never respond to messages that ask for your personal or financial details