Follow Up Calls Computer Software Service Fraud - 20.06.18

There is concern that victims of previous Computer Software Service Fraud (CSSF) are being re-targeted for "owed money". The National Fraud Intelligence Bureau (NFIB) reports that CSSF scammers are returning to contact previous victims, requesting that they pay money owed for a fake malware protection service they had provided. Alternatively, the fraudster will ask for a new subscription fee in return for protection from a new threat. The victims that have made payments to the fraudsters have done so via credit/debit card payments. In some instances threatening and aggressive language has been used against victims, as part of the attempt to coerce them into sending money.

Computer Software Service Fraud involves the victim being contacted, told that there is a problem with their computer, and that for a fee this issue can be resolved. The aim of the fraudster at this point is usually to gain remote access to the victim's computer and, subsequently, access to their online banking account. No fix actually occurs. The victims will often be cold-called or will receive a pop-up on their computer, prompting them to phone the suspect.

Since the beginning of this year (2018), the total loss for repeat victims of CSSF has been reported as £16,712.85. The National Fraud Intelligence Bureau has noticed an increase in such reports since the beginning of May.

Protect Yourself

- If you receive such an unsolicited call or pop-up, do not make a payment. Always ensure you know who you are talking to. If in doubt, hang up immediately.

- Do not allow remote access to your computer.

- Don't be rushed or pressured into making a decision. Under no circumstances would a genuine bank, or another trusted organisation, force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons. Remember to stop and take time to carefully consider your actions.

- Listen to your instincts. If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

For more information about how to protect yourself online, visit www.cyberaware.gov.uk and takefive-stopfraud.org.uk

If you have been a victim of fraud or cybercrime, report it to us at Actionfraud.police.uk, or by calling 0300 123 2040.

Message Sent By
Action Fraud (Action Fraud, Administrator, National)