

NOT PROTECTIVELY MARKED

National Fraud
Intelligence Bureau



Microsoft Tech-Support Scammers using WannaCry attack to lure victims

23/05/2017

Copyright © City of London Police 2017

NFIB Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this alert, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances or matches or contradicts or casts doubt upon any content published in this Alert, please contact the City of London Police NFIB by return.

ALERT

Action Fraud has received the first reports of Tech-Support scammers claiming to be from Microsoft who are taking advantage of the global WannaCry ransomware attack.

One victim fell for the scam after calling a 'help' number advertised on a pop up window. The window which wouldn't close said the victim had been affected by WannaCry Ransomware. The victim granted the fraudsters remote access to their PC after being convinced there wasn't sufficient anti-virus protection. The fraudsters then installed Windows Malicious Software Removal Tool, which is actually free, and took £320 as payment.

It is important to remember that Microsoft's error and warning messages on your PC will never include a phone number. Additionally Microsoft will never proactively reach out to you to provide unsolicited PC or technical support. Any communication they have with you must be initiated by you

PROTECTION / PREVENTION ADVICE

How to protect yourself:

- Don't call numbers from pop-up messages.
- Never allow remote access to your computer.
- Always be wary of unsolicited calls. If you're unsure of a caller's identity, hang up.
- Never divulge passwords or pin numbers.
- Microsoft or someone on their behalf will never call you.

If you believe you have already been a victim

- Get your computer checked for any additional programmes or software that may have been installed.
- Contact your bank to stop any further payments being taken.

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at

<http://www.actionfraud.police.uk/>

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: <https://www.surveymonkey.com/r/FeedbackSDU>.