**From Neighbourhood Watch - West Kent Division**

**Fraudsters are turning to kindness with new phishing emails which encourage the recipient to open an attachment on the false premise that they could have already fallen victim to scammers.**

In the past three days, Action Fraud has received 226 reports from email users who have this email. The phishing email is sent from a fraudster who describes themselves a “law-abiding citizen” and has accidentally received the email recipient’s personal details. Attached to the phishing email is a document which the fraudster claims contains the recipient’s personal details.

The fraudster suggests that the email recipient’s details may have been made available to scammers and they are contacting them to try to rectify the problem. To do so the recipient must open the document.

In reality, the attached document opens the door to malware being downloaded onto the victim’s computer. The malware attempts to obtain sensitive data from victims, such as banking credentials and passwords; this is subsequently used to take money from the victim.

In order to protect yourself from malware, having up-to-date virus protection is essential; however it will not always prevent you from becoming infected.

**Protect yourself**

* Don’t click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can ‘spoof’ an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication.
* Do not enable macros in downloads, enabling the macro will allow the Trojan/malware to be installed onto your device
* Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
* Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It’s important that the device you back up to isn’t left connected to your computer as any malware infection could spread to that too.
* If you think your bank details have been compromised, you should immediately contact your bank.