# Keep your money safe

Each month, we see many incidents of fraudsters targeting Sussex residents in an attempt to defraud them. Operation Signature is our answer to preventing and supporting vulnerable victims of fraud or scams.

By its very nature, fraud is constantly evolving and taking on new forms. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.

This month we focus our attention on phishing emails, protecting your pension pot and a payday loan company's data breach, so we offer advice on what you should do to protect your money.

**Detective Chief Inspector Steven Boniface, Operation Signature, Sussex Police**

## Identify phishing emails

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.

The phishing email is sent from a fraudster describing themselves as a 'law-abiding citizen' who has accidentally received your personal details. Attached to the phishing email is a document which the fraudster claims contains your personal details and suggests that your details may have been made available to scammers and they are contacting them to try to rectify the problem. To do so you are told you 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; although it won't 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. You can find out how by searching the internet for relevant advice for your email provider.
- Do not enable macros in downloads; enabling macros will allow 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 is important that the device you back up to is not connected to your computer as any malware infection could spread to that as well.
- If you think your bank details have been compromised, you should contact your bank immediately.

## Thinking of doing something with your pension pot?

Pension fraudsters are after your savings. They'll do whatever it takes to trick you – like cold calling, pretending they're from the government, or promising an amazing deal if you sign up straightaway.

If you're thinking of cashing in your pension, take your time and check everything for yourself. Don't take someone else's word for it.

Visit **pension-scams.com** run by the Pension Regulator and get to know the **five steps** you need to take to protect yourself.

Thousands of people have lost their life savings. Don't be next. Before you go any further, read the Pensions Regulator's **five tips** to protect yourself from fraudsters.
You can find them on the Pension Regulator website at:
**http://www.thepensionsregulator.gov.uk/pension-scams.aspx**

## Wonga (Payday loans) data breach

There has been an extensive data breach at Wonga (payday loans company); up to 245,000 UK customers may be affected.


**Be aware**

- If any of your financial details were compromised, notify your bank or card company as soon as possible. Review your financial statements regularly for any unusual activity.
- Criminals can use personal data obtained from a data breach to commit identity fraud. Consider using credit reference agencies, such as Experian or Equifax, to regularly monitor your credit file for unusual activity.
- Be suspicious of any unsolicited calls, emails or texts, even if it appears to be from a company you know of. Don't open the attachments or click on links within unsolicited emails, and never disclose any personal or financial details during a cold call.
- If you suspect you may have been a victim of fraud, attempted fraud or cyber-crime, please report it to 101.

**If you or someone you know is vulnerable and has been a victim of fraud call Sussex Police on 101 or visit www.sussex.police.uk**

OPERATION SIGNATURE
Protecting vulnerable victims of fraud

If you need to a report fraud or attempted fraud, you can do so by contacting Action Fraud at or by calling 0300 123 2040. You can also read the latest Action Fraud alerts at www.actionfraud.police.uk/news or by following @actionfrauduk on Twitter.