Keep your money safe

Sussex Police fraud newsletter – January 2018

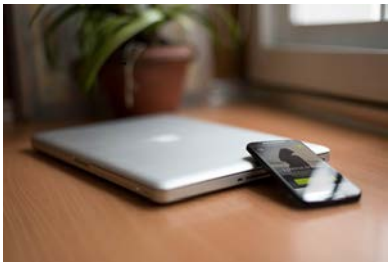
Each month, we see many incidents of fraudsters targeting Sussex residents in an attempt to defraud them. Operation Signature is our answer to preventing and supporting vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.

This month's newsletter provides advice on different types of online fraud to look out for – particularly when messages request something from you – from your bank to well established shopping websites. We also provide some preventative tips to take if you're booking a holiday.

Peter Billin, Detective Inspector, Economic Crime Unit, Sussex Police

NatWest 'smishing' alert

Smishing is a term for a message you think you have received from your bank or another organisation you trust, telling you there has been fraud on your account. They may ask you to deal with it by calling a number or visiting a fake website to update your personal details.



We have received reports of a range of **smishing** messages claiming to be from NatWest that lead to websites harvesting personal banking information. Specialist software is used which alters the sender's identification on the message to appear that it's from NatWest, adding it to any existing message threads on the recipient's phone.

If you already bank with NatWest and received legitimate messages from them in the past, this could easily catch you out. They are also targeting individuals regardless of whether they are customers of NatWest or not. If you click on the link that the message provides, you'll be taken to an exact replica of the NatWest website that asks for sensitive personal information including full name, address, contact details, PIN and debit card numbers. Banks **will never ask for all of your personal details** in emails or links, please don't provide them. Contact your bank using if you have any queries with your account.

Booking holidays

In the New Year, when you start looking to book holidays it can be a potentially dangerous time to fall victim to fraudsters.

Always consider the following preventative steps.

Top tips to avoid holiday booking fraud

- **Stay safe online**
  Check the web address is legitimate and has not been altered by slight changes to a domain name – such as going from **.co.u**k to **.org**.

- **Do your research**
  Do a thorough online search to ensure the company is credible. If they are suspect, other people may well have posted their experiences warning people off.

- **Look for the logo**
  Check whether the company is an ABTA member by looking for the logo on the company's website. If you have any doubts, verify membership by visiting the Find a Member section of the ABTA website. If you are booking a flight and want more information about ATOL protection, or would like to check whether a company is an ATOL holder, then please visit the CAA website.

- **Pay safe**
  Never pay directly into an individual's bank account. Paying by direct bank transfer is like paying by cash – the money will not be traceable and is not refundable.

- **Check the paperwork**
  You should study receipts, invoices and terms and conditions, and be very wary of any companies that don't provide any at all. When booking through a Holiday Club or Timeshare, get the contract thoroughly vetted by a solicitor before signing up.

- **Trust your instincts**
  If something sounds too good to be true, it probably is.

Warning on clicking links that look legitimate

We have had several reports in Sussex of people being sent emails from organisations such as Amazon and the Television Licensing Office. Recipients are asked to click on links to assist with a refund to be processed.

The links have subsequently asked for personal and bank details to be entered, resulting in victims losing considerable amounts of money from their bank accounts. We urge people to be very wary of clicking on any links from emails they've received and to not provide any personal details, especially those relating to their bank accounts.

If you suspect someone you know may be vulnerable to fraud, please share this newsletter with them and encourage them to look at the 'Little Book of Scams', available on the following link: http://tinyurl.com/z8khtgh.

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 www.actionfraud.police.uk/report_fraud 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. Check latest information online at www.getsafeonline.org.