A GUIDE FOR CONSUMERS:

Staying Safe When You Bank or Shop Online

Home Office

INTRODUCTION

This document sets out some of the common methods used by fraudsters to target members of the public when using online financial and retail services, as well as some common victim behaviours and simple safety tips for consumers using these types of services online. This report draws on real life, anonymised examples of crimes reported to Action Fraud[1].

The largest category of fraud offences recorded in the year ending September 2015 was banking and credit industry fraud[2]. Victims also commonly report to Action Fraud that they have been victims of online shopping and auction fraud.

ANYONE CAN BECOME A VICTIM OF FRAUD.

AND...IT IS A MYTH THAT YOU WILL ALWAYS GET YOUR MONEY BACK FOR ANY FRAUD OCCURRING FROM AN ONLINE TRANSACTION.

1 Methodology on page 6

2 ONS (2016) Crime in England and Wales, Year ending September 2015. UK: ONS. Available at: http://www.ons.gov.uk/ons/dcp171778_419450.pdf Accessed February 2016

PART 1: CRIMINALS – EXAMPLES OF HOW THEY GET THEIR HANDS ON YOUR MONEY

FAKE ADS! - "I TRUSTED IT BECAUSE IT WAS ON MY FAVOURITE SHOPPING SITE"

Just because you are on the website of a brand you trust, it does not mean that the adverts have been vetted by them – some Ads can contain malware (putting viruses onto your computer), and others are placed there by fraudsters.

CASE STUDY

Daniel wanted to buy a television and saw an advert for one on his regular electrical site. Clicking into the link, he ordered a television set and he was requested to send payment via bank transfer. After Daniel paid, he didn't hear anything else from them again. He lost £499.

SPOOFED BRANDS - CRIMINALS USE FAKE EMAILS AND TEXTS TO CONVINCE PEOPLE THAT THE EMAIL HAS COME FROM THE ORGANISATION THEY HAVE AN ACCOUNT WITH.

They might ask you to update your account details as a ploy to get your information. The email or text may also contain a link which could contain malware.

CASE STUDY

Paul received a normal looking email which appeared had been sent from a well-known company that he had an account with, advising him that he needed to update his details, so he followed the instructions and sent his details through. Shortly after, Paul discovered that he was blocked from accessing his other online retail accounts as the fraudsters had taken his original account details and changed all his passwords.

CASE STUDY

Mrs Sihan received a call from her bank who wished to discuss some transactions made on her business account. Her granddaughter Neena was suspicious and asked the caller to phone her mobile so she could see the caller ID and check the number. The number matched her bank's number. The caller advised that there had been several attempted transactions made on the business account which Mrs Sihan confirmed were not genuine and the caller reassured her that they had blocked these payments. However the caller then advised Mrs Sihan that her savings account had been hacked and that the money within the account needed to be transferred to a holding account to ensure it would be safe. Mrs Sihan went online and transferred a total of £40,000 before she called her bank to check and was then told that this was not genuine.

FRAUDSTERS - PRETENDING TO BE FROM YOUR BANK OR RETAILER

Most of us would not easily give our personal information away to strangers on the phone – but they can be very convincing and pretend to be from somewhere we trust. They can even call from a number which appears to be an official company number.

PART 2: VICTIMS – EXAMPLES OF HOW YOU CAN MAKE YOURSELF VULNERABLE

YOUR EMAIL ACCOUNT

Fraudsters want access to your financial details. One way to do this is to get into your email account, which holds the key to many others. They also know that people often have the same password for everything – so once they are in they can get to your other accounts.

CASE STUDY

Alex discovered that the password to one of his retail accounts had been changed without his authorisation, and soon after, his loyalty points were all used by an unknown person and he was blocked from accessing his account. Then Alex received a notification to say that his password had been changed on another of his retail accounts so he notified the company who took his account offline and then ensured he changed the password to both accounts.

ENSURE SOMEONE HAS REALLY PAID YOU BEFORE YOU GIVE SOMETHING AWAY

CASE STUDY

Michelle wanted to sell her oven and so advertised it on an auction site. She soon received an email from someone who was interested (Carol) who said that she would pay Michelle via a secure payment method. Michelle received an email from the payment company advising that there was £610 pending to go into her account, so when Carol asked for £104.90 to pay the shipping fees and insurance, Michelle paid this. But when Michelle contacted the payment company she was told the email which was supposed to be from them was not genuine. Michelle lost £104.90.

CASE STUDY

Tony was trying to sell his computer online and an interested buyer (Jason) said he would pay him direct by bank transfer and drop by Tony's house to collect it. When he arrived, Jason showed Tony a screen shot on his phone showing that the money had gone in to his account. Suitably assured, Jason then left with the item. However Tony never received the payment- it was a mock-up of his account.

CHECK BEFORE YOU SIGN FOR THINGS TO MAKE SURE IT IS WHAT YOU ACTUALLY ORDERED

CASE STUDY

Russell bought an iPhone 6 from a seller through an auction website account and paid for it via a secure payment method. However after the parcel arrived, when Russell opened it he found 2 spoons, an empty bottle of shampoo, scissors and a can opener. He could not trace the seller.

FRAUDSTERS MIGHT ASK FOR SOME EARLY PAYMENTS TO RELEASE THE SALE

CASE STUDY

Geoff needed a significant size loan and he applied for 30,000 US Dollars online from a small provider and his application was successful. However to secure the deal he was asked to pay the first instalment of £500 upfront so he made payment via an online payment method. Geoff was then contacted the next day by the loan company and asked to pay a further £1,250 for tax purposes within the UK which he paid, but then alarm bells rang. Geoff found out that a temporary account had in fact been opened in his name with a well-known bank.

BARGAINS.....THAT TURN OUT NOT TO BE

Bargains are always worth snapping up – or are they? If something is too good to be true, it often is.

CASE STUDY

Mrs Booker was emailed about the chance to win shop vouchers for her favourite store at a discount price. She entered in her details, then subsequently discovered that she was being charged for subscribing to a service she had never asked for and she did not want.

IT'S HARD TO SAY NO TO A REFUND.....OR UNEXPECTED EXTRA MONEY!

CASE STUDY

Vince was called from someone who claimed to be his internet provider advising Vince they have identified a fault with his computer. The caller requested that Vince switch his computer on and subsequently Vince gave him remote access so they could rectify the problem. The caller then offered Vince £200 refund for the inconvenience caused and asked Vince to access his online bank. Vince went onto his online banking and noticed that £4300 was put into his account instead of the £200. The caller confirmed this was a mistake and asked that Vince send £4000 back via an online payment method in Thailand which Vince did but then Vince realised that around £3000 had in fact been taken from his ISA and put into his current account, so he was in fact paying his own savings back to the caller.

PART 3: KEY SAFETY TIPS

BEFORE YOU START SHOPPING...

On your device:

TIP! **Make sure you create a strong password for your email account and all of your other online accounts**. A strong password can be created by simply choosing three random words to put together to create the password. **Do not use the same password for all of your accounts** and never use words that are related to you and can be easily guessed (i.e. your favourite sport, place of birth, town where you live etc.).

TIP! **Ensure that you have installed security software** such as antivirus which helps protect your devices from viruses and hackers.

TIP! **Always download the latest software updates** as soon as possible after you received them as these contain vital security upgrades which help keep your devices secure.

On the phone:

TIP! **Don't share personal information with people who call you– no matter where they say they are from**. Independently find a contact number for the organisation they purport to be from, then wait at least ten minutes for the phone line to clear and call that number to confirm if the organisation has been in touch.

TIP! **Do not be pressured into making any decisions or sharing any information**. Fraudsters give many reasons why you shouldn't stop the call-including that you are helping them with a fraud and cannot tell anyone. Banks will never ask you for your pin or full password over the phone. For more consumer advice on preventing fraud in the financial sector, visit: Financial Fraud Action UK: http://www.financialfraudaction.org.uk/consumer-advice.asp and British Bankers Association: https://www.bba.org.uk/customers/personal-banking/financial-crime-personal-banking.

TIP! **Do not share your online passwords with those who call you** – even if they say they are from your computer company.

Whilst shopping online:

TIP! **Beware of people offering you a deal below the current bid or reserve price**, especially if they contact you direct. Be especially careful when buying things from people with little or no selling history.

TIP! **Don't pay directly to individual sellers, only to a registered company or intermediary website**. Stick to the communications channels provided by the website, and use a secure online payment method, which helps to protect you. If possible, pay by credit card.

TIP! **Ensure that the locked padlock or unbroken key symbol** is showing in your browser before entering card details.

TIP! **The beginning of the online retailer's internet address will change from 'http' to 'https'** to indicate the connection is secure. **Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online**, which includes not only credit cards but some debit cards too. This adds an additional layer of security to online transactions with signed-up retailers.

TIP! **Be wary of accepting payment by cheque**. Even though it may clear, you are still liable if the cheque turns out to have been forged or stolen. Don't accept a cheque for a higher amount and refund the difference – this is a common tactic used by fraudsters.

TIP! **Check products before you sign for them** - they might not be what they are advertised as.

Spoof emails/texts:

TIP! **Don't reply immediately!** You can always call your bank/shop using the phone number on a genuine piece of correspondence or website to check if you're not sure. Banks and financial institutions will never send you an email or text asking you to click on a link and confirm your bank details.

Dodgy Websites/Adverts:

TIP! **Do not immediately clink into unknown adverts** – these can contain malware. Just because you can see an advert on a well-known trusted site, it does not mean that the site has verified the company in any way – they are completely independent. You will need to do your own research to confirm its credibility.

TIP! **Be cautious when paying by direct bank transfer**. Criminals often say that the secure online payment method failed and ask you to pay by direct bank transfer instead. However, unless you pay on a credit card, you have no security. **Remember that sharing payment information via email is not secure** – don't do it!

TIP! **Check the URL in the web browser**. A tactic often used by fraudsters is to change the address very slightly. For example a real address such as '. . . @COMPANY.com' could be changed to '. . . @COMPANYS.com'.

For more advice and helpful tips on how to stay safe online, visit the below:

- Action Fraud http://www.actionfraud.police.uk/fraud_protection/online_shopping and http://www.actionfraud.police.uk/fraud_protection/identity_fraud provides specific advice on online shopping and identity theft
- Cyber Streetwise https://www.cyberstreetwise.com and Get Safe Online https://www.getsafeonline.org both provide advice for individuals and businesses
- FFA UK http://www.financialfraudaction.org.uk
- British Bankers Association https://www.bba.org.uk

PART 4: KEY FACTS

The online economy is growing fast - the average weekly spend of UK customers online in October 2015 was £839.1 million, 11.2% more than the same time in the previous year[3].

Use of internet banking has also nearly doubled in less than ten years, from 30% of users in 2007 to over half (56%) in 2015[4]. The ability to shop online and make payments without having to leave your home brings clear benefits for us all, but it also opens us up to new risks.

During the year ending September 2015, fraud offences accounted for 14% of Police Recorded Crime.[5] There were 604,601 fraud offences referred to the National Fraud Intelligence Bureau (NFIB) during the year ending September 2015; an increase of 5%, compared to the year ending September 2014. The largest category (56%) of fraud offences recorded by the NFIB in the year ending September 2015 was banking and credit industry fraud with 339,529 offences recorded – an increase of 8% compared to the year ending September 2014. There were also 40,363 offences recorded in the same time period relating to online shopping and auction frauds.

Internal analysis of fraud reports by the National Fraud Intelligence Bureau indicates that approximately 6% of fraud victims between April 2014 and March 2015 had been a victim before.

Methodology

The case studies in this report are drawn from a random sample of crime reports made to Action Fraud by the public over a period of six months (May- Oct 2015), which were believed to include reference to one or all of twenty-two well known online retailers and retail banking groups selected for this study. The data set relied on information provided by the victim only. This can mean that some details are missed, left incomplete or the true context of the crime is misinterpreted. However, these cases provide a snapshot of the ways that fraud can occur online, giving a useful insight into criminal techniques and how you can protect yourself. The names of the people used in the case studies are entirely fictitious.

3 ONS (2015) Retail Sales, October 2015. UK: ONS. Available at: http://www.ons.gov.uk/ons/dcp171778_424664.pdf Accessed November 2015.

4 ONS (2015) Internet Access – Households and Individuals 2015. UK: ONS. Available at: http://www.ons.gov.uk/ons/dcp171778_412758.pdf Accessed January 2016.

5 ONS (2016) Crime in England and Wales, Year ending September 2015. UK: ONS. Available at: http://www.ons. gov.uk/ons/dcp171778_419450.pdf Accessed February 2016