Digital Safety

2018

NatWest

THE : FUTURE : LABORATORY

THE FUTURE OF FINANCIAL FRAUD

Financial fraud is now the most common crime in the UK. With a growing number of people using remote banking – which comprises internet, phone and mobile - opportunities for fraudsters to find ways to defraud money out of hard working people are set to boom.

Remote banking fraud totalled £73.8 million in the first half of 2017, a 3% rise from the same period of 2016. This fraud typically involves customers being tricked into revealing their security details through scam phone calls, texts and email, or details obtained through malware, which are then used to access a customer's online account.

While losses due to internet banking fraud fell by 1% in the first half of 2017 to £55.5 million, the number of cases increased by 5%, and losses due to mobile banking fraud are increasing. They totalled £2.6 million in the first half of 2017, marking a 19% rise on the same period in 2016.

Consumers, the banking industry and the government must remain vigilant if they want to drive down financial crime.

Staying several steps ahead of the fraudsters is crucial to prevent further theft.

This report takes a detailed look at the new fraud we can expect to see increase in 2018 – and beyond – and how consumers can best protect themselves

SCAM SCENARIO 1: Social media spying

According to Charlie Cadywould of think tank and research institute, Policy Network, throughout 2018, we can expect to see an increase of financial fraud that directly targets consumers in a personalised way. Fraudsters will use all means available to them and target consumers in evermore sophisticated ways, using the seemingly benign information consumers share on their preferred social media platform be it Facebook, Twitter or Instagram.

With the rise of social media, it has become commonplace for us to share everyday moments – big or small – with friends, family and followers. These snippets of information shared – whether it's a utility provider with terrible service or sharing news about an upcoming house purchase – can allow a fraudster to build up a tapestry of a person's life, their movements, and the businesses they use.

Traditionally, fraudsters would pose as someone from a bank or building society, with the intention of extracting bank details. Typically, a victim will receive an email (phishing) or text message (smishing) asking to click a link or call a phone number to verify log-in, account and password information. The customer is then taken to a malicious site that looks like the bank's genuine login page. If the customer logs in from this page, the fraudster is able to access their information which could lead to current and savings accounts being compromised. Other cases involve a phone call (vishing) where a fraudster will pose as someone from an organisation with a ready-made story that will lead to the victim revealing their details.

Victims fall for such tales because criminals make sure they know enough information to appear genuine. But social media has dramatically changed this, making it easier than ever for fraudsters to find out who customers bank with or which gym they use.

Julie McArdle, NatWest Security Manager said:
"People can be very liberal with posting information on social media. They might not realise how much they're giving away. But to a fraudster the posts can be very informative – and they will use these details to earn trust. They can be incredibly convincing."

EXAMPLE 1:

YES! Mortgage approved on our dream home. One step closer to completion and #movingday"

Sharing good news on social media to keep loved ones updated on important moments is now commonplace and fraudsters will use this to their advantage.

This year, we can expect to see fraudsters push social media stalking to the top of their agenda, keeping their eyes peeled for anyone sharing information about an event that is likely to mean the person will have some money swilling around.

For example, a fraudster might spot this news about someone moving to a new house and know they will be receiving house proceeds from their bank or mortgage provider. This could result in the fraudsters impersonating their solicitor and requesting for funds to be misdirected to them.

EXAMPLE 2:

"Absolutely sick of the terrible service from @BroadbandCompany. Definitely going to change"

By simply noticing a social media post about an internet provider, a fraudster can call and pose as a member of staff from the mentioned provider. To a customer (their victim) they would most likely expect the caller to be genuine.

They might draw attention to a fake security breach of an internet connection and take remote access of someone's PC to resolve. They will ask the customer to log-in to their online banking whilst they have remote access and to leave the PC whilst they fix the 'issues'.

Or, during the conversation, a fraudster will recommend the customer share their authorisation codes to process a refund. This provides the fraudster what they need to set up a payment away from the customer's account.

How to beat the criminals:

- Customers should be cautious with what they disclose on social media. Customers should ensure that their profile is private and only viewable to people they know.
- Just because someone knows a customer's basic details (such as name, address or mother's maiden name), it doesn't mean they are genuine.
- Customers should be cautious of any unexpected calls from companies that they use. If in doubt it's always best to hang up the call and call the company on a trusted number.
- A bank will never ask a customer to move money for security reasons.
- Protect PCs and laptops with up to date anti-virus and anti-malware software.

Julie McArdle, NatWest Security Manager said:

"Remember that a bank or the police will never call a customer and request a full online banking password. Equally, nor will any utility companies or internet providers. Unless you have given third party consent, the only person who should have knowledge of a customer's security details, including PINs, passwords and authorisation codes, is the customer themselves.

The national campaign "Take Five to Stop Fraud", which launched in October 2017 helps customers protect themselves from fraud. It is focused on helping consumers to recognise fraud and confidently challenge any requests for their personal or financial details by remembering the phrase 'My money? My info? I don't think so'. Visit: https://takefive-stopfraud.org.uk

SCENARIO 2: Malicious software on smart phones

Criminal gangs use malware - malicious software that is unknowingly downloaded onto a device - as a means to compromise customers' security and personal details. Malware enables criminals to spy on victims' browsing habits and can even give its controllers total control over a device.

Up until now, malware has been most prominent on PCs and laptops, but consumers should now be prepared for criminals to target their smartphones.

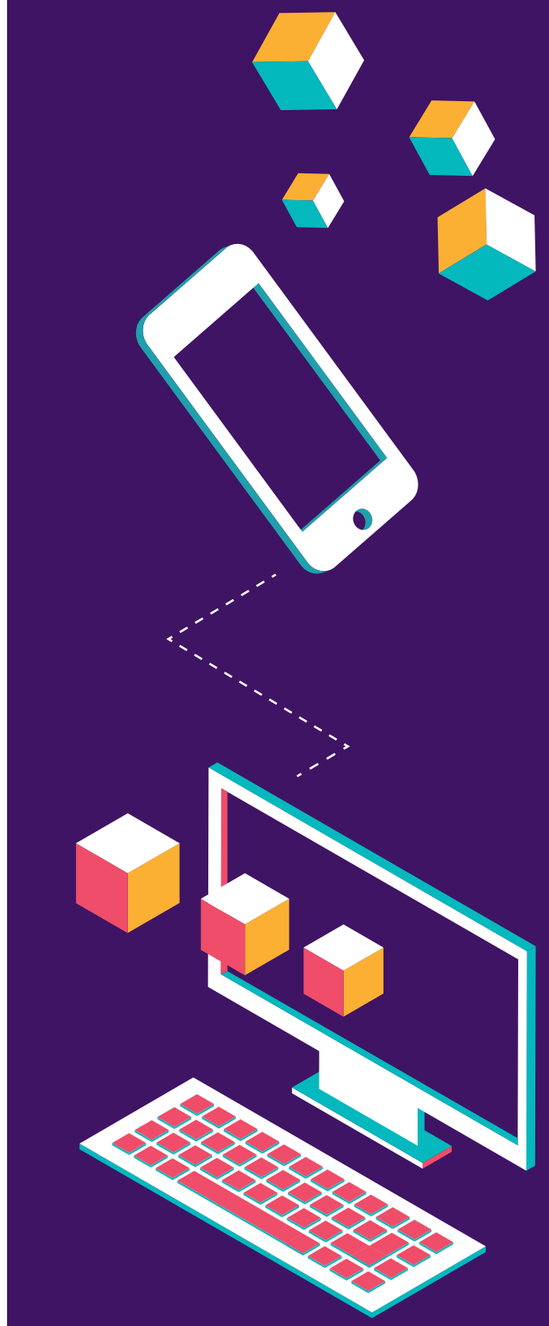
Jane Howard, Managing Director of Personal Banking at NatWest said: "An emerging threat is how malware will manifest in mobile banking on smartphones. I suspect that this will become more prominent as time passes as we see it as a real threat right now on desktop devices such as PCs and laptops. We are continually investing in the security of our mobile banking app to ensure malware is ineffective at compromising it."

EXAMPLE 1:
By spying on a mobile phone user, criminals can see log-in and password details that can subsequently be used to access customer accounts and to commit fraud.

EXAMPLE 2:
In taking over a device a fraudster can move money freely out of accounts and into their own.

How to beat the criminals:

- Customers should keep their mobile devices' operating systems up to date to ensure that they have the latest security patches and upgrades. Older software may have security vulnerabilities that could expose the device to additional risks.
- Think carefully before jailbreaking or rooting a device as it may weaken security and expose it to additional risks. Jailbreaking/rooting is when someone changes the security settings of a phone to allow the downloading of 'unofficial' apps that are not available from the app store.
- Only download apps from official app stores such as Apple and Microsoft App stores and Google Play.



ONE TO WATCH: MONEY MULES

As salaries fail to keep up with inflation, and unemployment is rife in certain parts of the country, more people are going to be looking for better paid work - and more likely to respond to job adverts, or social media posts that promise large amounts of money for very little work. Criminals need foot soldiers to move money and prey on cash-strapped households.

Mule recruiters trawl job sites or social media for potential targets. In particular, they look to target cash-strapped students by visiting university towns or placing targeted ads on Facebook. Money mules are recruited by criminal gangs to transfer stolen money between different bank accounts. Money mules receive the stolen funds into their account, they are then asked to withdraw it and wire the money to a different account, often one overseas, keeping some of the money for themselves.

Customers should never accept any offer of quick and easy cash and should always follow their bank's security advice. Accepting payment for receiving money into your account and sending it on to another is the main activity of a money mule and is a criminal offence. It is very likely money laundering and can result in your account being closed by your bank, making it very difficult to open another account with another UK bank. Money mules can also face prison sentences of up to fourteen years.

MORE POTENTIAL FRAUD AND SCAMS TO WATCH OUT FOR IN 2018

EXAMPLE 1: BREXIT

Criminals are likely to use the uncertainty of Brexit to their advantage and consumers should be prepared to thwart attempts from fraudsters using the UK leaving the EU to push fake investments.

The scam: Scammers are playing on current economic uncertainty to pressurise victims into putting their savings into bogus investments. Equally they could use the opportunity to send emails with sensational headlines about Brexit to encourage recipients to click on a link that will download viruses and spyware.

How to beat the criminals:

- Customers should reject unexpected offers that seem too good to be true. If a company is establishing contact out of the blue (via a cold call or email) it is likely either high risk or a scam.
- Avoid being pressured to invest quickly. Scammers may offer fake bonuses or discounts for handing over money fast.
- Almost all financial services firms must be authorized by the FCA. You can check the Financial Services Register to check if a specific company is on the list.
- Check if a specific investment or pension opportunity is on the FCA warning list here: https://www.fca.org.uk/scamsmart

EXAMPLE 2: ROMANCE SCAMS

More than 16 million people were using dating apps in 2017 and this number is set to increase in 2018 with the popularity of datings apps showing no signs of slowing. Criminals know this and will be infiltrating these apps in 2018.

Action Fraud, the UK's cyber-crime reporting centre, says it already receives more than 350 reports of dating scams a month. Users should be on their guard this year.

The scam: Criminals create fake profiles to form a relationship with their victims. They use the quick messaging functionality to quickly (and subtly) mine personal details – where a customer lives, a pets name, favourite sports team – when they have enough they could use this information to steal the customer's identity and open credit cards and loans in their name.

Alternatively, they work to build a trusted relationship with their victim. Just when the victim thinks they've met the perfect partner the scammer asks for money - sometimes to help with a problem. This problem could be a sick family member or they need money for medical treatment. They might even ask the victim to pay for their travel to come and visit.

How to beat the criminals:

- Customers should never send money to someone they have never met.
- Personal financial details, such as credit card details or statements and personal ID, such as a passport or a driver's license should never be shared with someone you don't trust.
- Spelling and grammar mistakes, inconsistencies in a person's background and only seeing static pictures of a person can all be signs that someone orchestrating a scam.

EXAMPLE 3: FIFA WORLD CUP 2018

Football fanatics will be desperate to get hold of tickets to matches in Russia this June and July for the World Cup. Tens of thousands of loyal fans will be hoping to head to Russia - and looking for bargain tickets and travel companies to get them there. Crooks are poised to flood the market with fake tickets and trips during the second tranche of ticket sales in March and beyond.

The scam: Fans have been warned that some sites will sell tickets that are either fake – or will never arrive. It is also expected that fake package trips to Russia will be sold by fake travel companies that will see people end up with no trip - and their money disappeared into the pockets of criminals.

How to beat the criminals:

- Scammers may offer tickets on a legitimate site but direct customers to another site for payment. This is an indicator of a scam and customers should never do this.
- Customers should thoroughly research any site they are considering making a purchase through.
- Spelling and grammar mistakes, inconsistencies in a person's background and only seeing static pictures of a person can all be signs that someone orchestrating a scam.

ON THE RISE – ONLINE FRAUD USING A DEBIT CARD/CREDIT CARD

The rise of shopping online has given fraudsters new opportunities to take advantage of customers. Malware and innovative fraudsters could find ways to obtain card information that then allows them to make purchases with the details – this type of case is currently on the rise. Being aware of a few tips for keeping safe when shopping online can make a big difference:

- Only shop on secure and trusted websites and check for a padlock symbol displayed in the browser to show your information is handled securely.
- Customers can download NatWest's free security software IBM Rapport that protects card details online.
- Keep all PCs updated with the latest browsers and protected with anti-virus software.
- Customers should keep contact details, including a mobile number, updated with their bank.

EXAMPLE 4: ROYAL WEDDING FEVER

The excitement that will build in the run up to the wedding of Prince Harry and Meghan Markle, on Saturday 19th May, will spark couples, all around the UK, to bag a date in the same year. More than 600 wedding day frauds and scams were reported to police in six months alone during 2017. Criminals routinely scam happy couples planning a wedding and will be ready to swoop on those getting married this year.

The scam: As the cost of weddings increases, experts fear couples are becoming easy prey for criminals who tempt victims with extravagant offers at bargain prices. Scams will relate to venues, catering, dresses and other services sold online. Scammers can set up fake websites within minutes for venue hire that can look exactly like the real thing. Further, fake wedding planners routinely take victims' money and disappear into thin air. Wedding dresses are another target for fraud – with many brides emailing their measurements in the belief they are ordering a bespoke garment which turns out to be from a Chinese online marketplace costing less than £100.

How to beat the criminals:

- Customers should shop around to make sure they're not paying an inflated price for goods that can be bought cheaper elsewhere.
- All suppliers should be fully investigated and customers should always double check any payments being made are going to the intended party.
- Customers could consider using suppliers that have been endorsed by a trusted third party. Check with family members and close friends for genuine providers.

EXAMPLE 5: GETTING ON THE HOUSING LADDER

First-time buyers are desperate to own their own home, but as first-timers they are inexperienced in the property-buying process. Criminals are at the ready to steal their hard-earned deposits.

The fraud: A computer hacker monitors emails sent by a solicitor and a homebuyer. When a bank transfer is about to be made, typically for a deposit, they pounce. The fraudster emails the homebuyer pretending to be the solicitor, telling them that the details of the law firm's bank account have changed. Many victims are told that the account is being "audited" and so another one must be used. The unsuspecting homebuyer sends their cash to the new account, where it is withdrawn by the fraudsters.

How to beat the criminals:

- When transferring large sums of money, customers should double check the details with the solicitor by calling their usual contact.
- Always be cautious if a third party's bank details change just before a large payment.

Top tips to remember when banking online

- **Requests to move money:** A genuine bank or organisation will never contact a customer out of the blue to ask ask them to move money to another account. Customers should only give out personal or financial details to use a service that they have given their consent to, that they trust and that they are expecting to be contacted by.
- **Clicking on links/files:** Customers shouldn't be tricked into giving a fraudster access to their personal or financial details. They should never click on a link in an unexpected email or text.
- **Personal information:** Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- **Up to date protection:** Protect PCs and laptops with up to date anti-virus and anti-malware software.