M&S BANK

PROTECT YOURSELF FROM FINANCIAL FRAUD

It pays to stop and think

In the first six months of 2018, over 34,000 people were scammed out of £145.4m

At M&S Bank, we work hard to keep you safe from fraud.

However, with more and more people being targeted by fraudsters, it's important to understand more about this crime and how to spot a potential scam. Taking the time to stop and think about a situation may help you to make the right decision in those crucial moments.

Fraud can happen at any place and any time. It could happen when:

- You're at home and receive a call to message asking you to call a number urgently urgently transfer money out of your account
- You're in a restaurant and receive a text message asking you to call a number urgently

Fraudsters look, sound and act like the bank, police or even your internet provider.

Fraud can happen in any place and at any time

Here's an example:

You're at home watching TV and receive a call from someone who says they're from your bank's fraud team.

A bank would...

... explain that there's been some unusual activity on your account and check to see whether you've made the payments. If not, they will stop the payment, cancel your card and order you a new one.

A fraudster might...

... ask you to log into your internet banking account and transfer funds to another account for safekeeping. They may ask for your PIN, or online banking passwords and security details.

A bank can already transfer funds at your request and would never ask for your passwords or PIN.

PHONE SCAMS

Phone fraud – or vishing – is when a fraudster calls pretending to be your bank or another trusted organisation. They can even make their phone number look like a number you know and trust.

They can sound very convincing and may already know some of your personal information, such as your account number or address. If you feel uncomfortable, or sense something is wrong, don't be afraid to end the call. You can always call the organisation on a number that you know, such as the number on the back of your bank card.

Fraudsters can keep the line open and even spoof a dial tone, so try to use a different phone, or wait at least 10 seconds before making your call. You could also call a friend or relative first, to make sure a fraudster isn't listening in when you do make the call.

Typical examples of vishing

- The Police or National Crime Agency need your help to solve a crime or ask you to move your money to a "safe account"
- Your bank need your help to investigate a fraud
- Your internet provider calls you to fix a problem you haven't reported
- HMRC threaten jail unless unpaid taxes are paid immediately

TEXT SCAMS

Text message fraud – or Smishing – is when a fraudster sends you a text that appears to be from your bank or another organisation that you trust. They may tell you that there's been fraud on your account and ask you to share or update personal details. The text may offer vouchers, a tax refund or ask you to confirm the delivery of a parcel.

Here's an example:

You're in a restaurant and receive a text message asking you to call your bank urgently. You call the number given and are told that there's been suspicious activity on your account. They ask if you've made the payments.

A bank would...

... stop the payment, cancel your card and issue you with a new one.

A fraudster might...

... ask you for your password, PIN, account number or sort code in order to stop the payment.

Typical examples of smishing

- Your bank tells you that your internet banking access has been restricted and asks you to click on a link to reinstate access
- Your bank asks you to move your money to a "safe account"

2 EMAIL SCAMS

Also known as phishing, emails are sent by fraudsters to encourage you to share personal details or to click on fake links. Take a few minutes to check whether the email seems genuine or not.

Here's an example:

You're at work and receive an email that appears to be from your bank.

A bank would...

...email you to tell you more about their savings accounts, mortgages or other accounts and services that they feel might be useful to you.

A fraudster might...

...email you asking you for personal details or information about your bank accounts.

Typical examples of phishing

- HMRC email to say you're owed a tax refund
- You win a lottery you haven't entered
- The Telephone Preference Service ask you to pay for a lifetime subscription

SIGNS OF AN EMAIL PHISHING SCAM

- You are asked to make an urgent payment.
- The sender's email address doesn't match the website address of the organisation it says it's from – hover your cursor over the sender's name to reveal the true address.
- It asks you to share personal information.
- Links in the email are not official addresses, i.e. marks&spencer.co.uk. Hover over the link to reveal its true destination.

£↑ INVESTMENT SCAMS

Investment scams claim to offer high returns for very little risk. Fraudsters often use false testimonials, fake celebrity endorsements, spoof websites and other marketing materials to make the scams appear genuine. If it seems too good to be true, it generally is.

Ways to spot an investment scam

- You're approached by phone, email, text message or by someone calling at your house with an investment opportunity
- The 'company' contacting you won't allow you to call back
- You feel pressured into making a quick decision, for example if the caller states the offer is "only available right now" or "don't miss out"
- The only contact you're given is a mobile phone number or a PO box address
- It seems too good to be true – high returns for a low risk

ROMANCE SCAMS

Somebody you have never met in person falls in love with you... and then asks you for money.

Typical examples of this would be

- Relative needs an urgent operation and has no health care
- They have a large inheritance and are unable to access the money
- Don't have any funds to travel to the UK (with promise of marriage)

ONLINE SCAMS

Online fraud is on the increase. Fraudsters use sophisticated tactics to access your financial details and passwords, creating bogus links and retailer web pages, as well as fake pop-ups.

Protect yourself from online fraud

- Always update the operating systems on your tablet, smartphone and computer as soon as they become available
- Install anti-virus software from a well-known and trusted company
- When shopping online, always check that the website you are using is genuine and when entering your personal or payment details ensure that there is a padlock in the address bar that indicates that your connection is secure
- If you're buying something online and you don't know the seller, never pay by bank transfer. Always use a credit card, debit card or PayPal – or a payment option that offers some protection against fraud

ACCOUNT TAKEOVER FRAUD

This growing crime is a form of identity theft, where a fraudster gains control of a victim's bank or credit card account and then makes unauthorised payments.

How this could happen

A fraudster calls, impersonating your internet provider. They tell you that you have some connection problems. To fix the problem, they ask you to log onto your computer and download a specific piece of software.

This software allows the fraudster to see your screen. They then ask you to log into your online banking account. The fraudster now has the opportunity to steal your banking details and move money out of your account.

An example of account takeover fraud

- The caller offers you a refund and 'accidentally' sends you too much money and asks you to return the overpayment. This creates a new payment to the fraudster on your account and now the fraudster can transfer money from your account to their account.

✓ **Always question uninvited approaches**

Instead, contact the company directly using an email or phone number that you can check is genuine.

✓ **Don't share personal information**

Never reveal your password or share your card details over email. Check the address of any website you're on. Be careful with the level of detail shared on Social Media sites and check your privacy settings.

✓ **Update your passwords**

Try to change your passwords at least twice a year. Don't use a password that can be easily guessed and make sure that your Online Banking password isn't the same one you use for other websites.

✓ **Check bank statements regularly**

If there are any transactions that you don't recognise, always contact us.

✓ **Check your credit report**

If someone has used your name to take out a loan or credit card, it may not show on your statements. Check your credit report at least once a year for any unusual activity.

✓ **Regular updates**

Always update your computer, tablet and smartphone operating systems as soon as they become available and install anti-virus software.

✓ **Shred important documents**

Shred any paperwork that reveals personal information, such as bank statements, card details and other sensitive data.

✓ **Register for Voice ID**

This is an additional layer of security that protects your account and makes it easy for you to call if you have a problem – no passwords to remember.

At M&S Bank we would never

- Phone and ask for your PIN or password, even by tapping them into your phone keypad.
- Ask you to provide numbers to us over the phone from an e-mail, text message or from your secure key.
- Ask you to transfer money into another 'safe' account in your name – even if we suspect fraud.
- Ask you to withdraw money to hand over to us for safekeeping.
- Send someone to your home to collect cash, your PIN, cards or cheque books, even if you are a victim of fraud.
- Ask you to pay for goods using your card and then hand them over to us for safekeeping.

If you're worried about fraud on your account, visit our security centre at bank.marksandspencer.com/security/, pop into your local branch or call us on 0345 900 0900.

TAKE FIVE TO STOP FRAUD™

For more information on fraud, visit
www.financialfraudaction.org.uk
www.takefive-stopfraud.org.uk

MSB8947-01/0519/WEB