Security matters

We're working hard to protect you against fraud but we can't do it alone. Find out more about the different types of fraud and how you can protect yourself.

We all think fraud is something that happens to other people, until it happens to us.

The truth is, we're all equally susceptible but we believe we're better protected when we work together to combat fraud.

We've been hard at work developing tools and techniques that make banking safer, but it's not enough. We need your help. If we all work together and follow a few simple steps, we can be better protected and keep your money safe – and that's good for everyone.

It's important to remember that we will never ask...

- Your PIN or full password, even by tapping them into your phone keypad.
- You to share a security code you've generated on your M&S PASS.
- To move money to another 'safe' account in your name – even if we suspect fraud.
- To withdraw money to hand over for safekeeping.
- To pay for goods using your card and then hand them over to us for safekeeping.

How can I protect myself?

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 Internet Banking password isn't the same one you use for other websites.

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. Be careful with the level of detail shared on social media sites and check your privacy settings.

Stay safe online

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

Shop safe online

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.

Check bank statements regularly

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

Shred important documents

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

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.

Email scams

Email scams – or phishing – are when a fraudster sends you an email, encouraging 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.

Clicking on a fake link may result in you being targeted in different ways, like a phone call from your bank's fraud department or more special offers.

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 that an email may be a 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. Hover over the link to reveal its true destination.
- You receive an offer of money, such as the lottery win you haven't entered or a tax refund from HMRC.

Text scams

Text scams – or smishing – are 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 you receive a text message saying that a payment has been set up on your account from a new device and to click on a link if it wasn't you.

A bank would...

... Ask you to call to confirm the transaction.

A fraudster might...

... Capture your Internet banking log in details from the spoof website attached to the link.

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".

Phone scams

Phone scams – or vishing – are 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.

Fraud can happen at any place and any time and the fraudsters often look, sound and act like the bank, police or even your internet provider.

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, PIN or M&S PASS security codes.

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.

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.

Visit the FCA website where there is an approved list of companies and a known scammers list together with more useful tips on staying safe.

Always call the Company on the number provided on the FCA website to verify that you are dealing with the genuine Company.

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.

A bank would...

...access your computer if YOU call the bank and it was necessary in order to help you.

A fraudster might...

...call and gain access to your account by impersonating someone you trust, like your bank or internet service provider.

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 the fraudster's account.

E-mail interception scams – payment/invoice diversion

Criminals monitor e-mail traffic and when payments are due they send their own e-mail that looks and feels like a genuine message from the company. They tell you that the bank details for your payment have changed and give you the new details to send your payments to. This could be a house deposit to your solicitor or a business customer's supplier. Always check with the company on a known genuine number before making payments to new bank details.

Take Five is a national campaign offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

If you're worried about fraud on your account, visit M&S Bank website security pages marksandspencer.com/security or call us on 0345 900 0900.

For more information on fraud, visit:
takefive-stopfraud.org.uk
getsafeonline.org

Please call 0808 001 1111 if you would like to receive this information in an alternative format such as large print, Braille or audio.

M&S Bank is a division of HSBC UK Bank plc. M&S is a registered trademark of Marks and Spencer plc and is used under licence. HSBC UK Bank plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register number: 765112). HSBC UK Bank plc is a company incorporated under the laws of England and Wales with company registration number 9928412 and its registered office at 1 Centenary Square, Birmingham, B1 1HQ. © HSBC Group 2026. All rights reserved.

Z0251/0626