What should I do next?

If a fraudster has your details then they may have used them to apply for credit with other business organisations in your name.

Consider contacting a credit reference agency. They will be able to offer you information and advice on identity and impersonation fraud and provide useful advice on how to protect your identity

You may also find the Identity Fraud website **www.identityfraud.org.uk** a useful source of information about identity fraud and impersonation.

Credit Reference Agencies

Experian Ltd
Tel: 0844 481 0800
www.experianreport.co.uk

Equifax
www.equifax.co.uk

Callcredit Ltd
Tel: 0870 060 1414
www.callcredit.co.uk

30 day free trial

Experian, the UK's largest credit reference agency, in conjunction with Vodafone, are currently offering a 30 day free trial of their **ProtectMyID service**. This service will help you make sure that your identity is protected from any further fraudulent attempts and they can offer you useful advice on what else you can do to protect yourself. To find out more about this service, contact Experian on **0844 481 81 91** today.

Please share this leaflet with your friends and family, so they can help to protect themselves too.

Don't be fooled

Staying safe from online scammers

Criminals may try to trick you into revealing personal information by pretending to be from a legitimate source – this is called 'phishing'.

A phishing scam usually begins with an email (with maybe a link to a fake website), a text or an unexpected call, which looks, sounds (and even really feels) like it's from a genuine business. The email or website might even have all the right logos or fonts on it.

The scam will ask for personal details like usernames, passwords and PINs – even bank account details!

So what do you do next? The first thing to do is – **nothing.** Don't reply to the email. Don't click on the link. And definitely do not enter and submit any of your personal details. Always delete a phishing text as it could infect your device with a virus.

WHO Rev 09/12

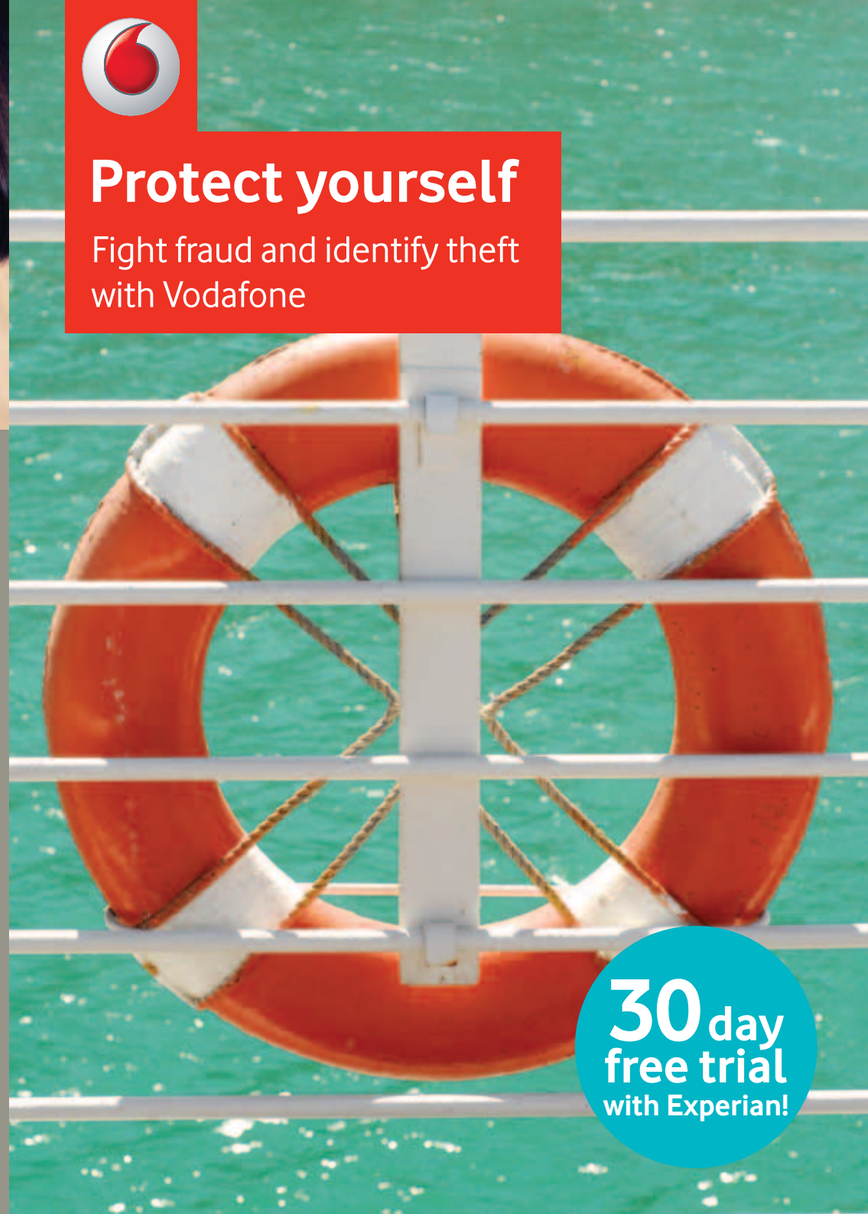
How to spot a phishing scam

Phishing isn't always easy to identify. Look out for things like:

- **Poor spelling** – those committing scams often have weak English language skills
- **Non-personal address** – the scammer probably doesn't know you by name, so they might address you as 'Dear Sir/Madam' or similar
- **Genuine email address** – at a glance, fraudulent emails can look like they're from a genuine organisation, but you should always double check the email address as it might have a letter out of place, which could easily be missed
- **The URL/web address of any links** – check that it's genuine, isn't unusually long and doesn't include special characters or letters substituted by numbers
- **Requests to act fast** – you'll often be urged to take action immediately, otherwise your account will be suspended
- **Unexpected email** – try to think if there's a good reason for this business to be contacting you

Protect yourself

Fight fraud and identify theft with Vodafone



30 day free trial with Experian!

You only get one identity...

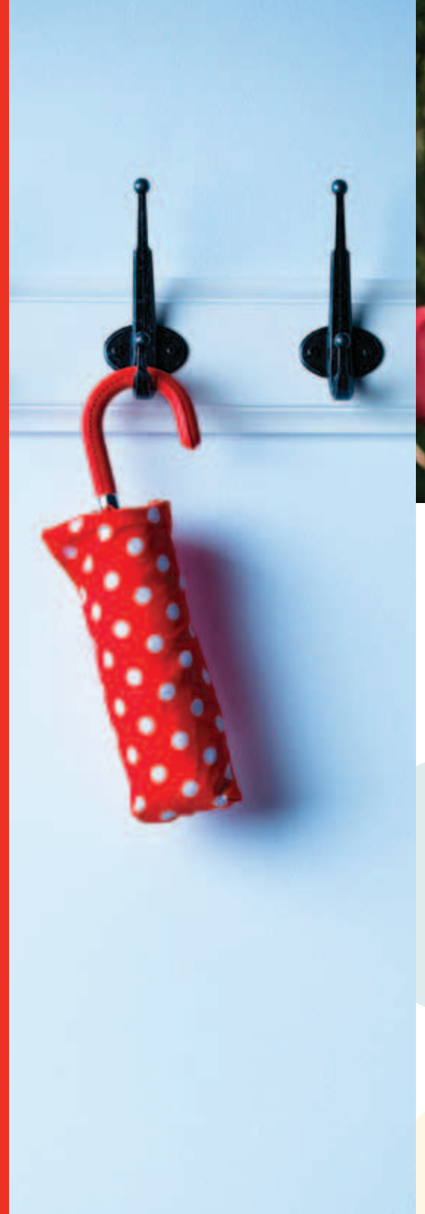
You don't realise just how important your identity is to you, until it is stolen. It can be an upsetting and worrying experience when you realise you might not be the only person using your own details.

At Vodafone we're dedicated to preventing fraud, but sometimes fraudsters do manage to open accounts in innocent people's names.

We are extremely concerned that this has happened to you and we are on the case to put things back to normal for you as soon as we possibly can. Now that we have closed down your Vodafone account we would recommend that you check your bank account and credit card statements and if you find you've had any money taken in relation to this mobile phone account, then please contact your bank or credit card immediately. They will be able to reimburse you directly via the banking industry Indemnity Claim process. If your bank account details have been compromised, your bank will advise you of the necessary steps to protect your accounts.

Within this leaflet you will find some help and guidance on the steps you can proactively take from now on to protect yourself and help keep your identity safe.

If we all work together, then we will have the best chance of beating fraudsters and stopping them in their tracks.



Here's some other ways you can protect yourself

Never

Never share your passwords or PIN numbers with other people and make sure they're not easy to guess

Shred

Shred any documents that contain your personal details before you throw them away

Check

Check the validity of anyone asking for your personal information. Don't be afraid to question them

Check

Check your bank, credit card and other financial statements for anything you might not have bought yourself

Always

Always be cautious if anyone rings you or emails you asking for personal information. If you are suspicious, offer to contact them directly instead

Limit

Limit the amount of personal information you share on social networking sites – and make sure you have full privacy settings in place

Keeping your mobile secure

Keeping people connected is what we do here at Vodafone, so even though you may not be a customer of ours currently, we still thought you might like to see the advice we offer our customers on how to keep their mobile secure.

Whether you use your mobile phone or device to download the latest apps, browse online or catch up with your social network, it's more important than ever to know how to keep data on your mobile secure:

Never allow applications or files to be installed from unknown sources (e.g. for Android apps outside of Google Play™)

Set up a password or PIN on both your phone and your SIM card – and keep your phone or device locked when you're not using it

If you go on a mobile website and the URL looks suspicious, close it straight away and do not download anything

Never store personal details like passwords or PIN numbers in texts or emails

If you sell your phone or give it away make sure that you do a factory reset to clear all of your personal data

If your phone or device is stolen, tell your service provider straight away – they will be able to block it to make sure it can't be used by anyone else

Voicemail security

It's really important that you set up a PIN for your voicemail inbox, so only you can access it – and never, ever share it with anyone. Ask your service provider for details on how to do this.