Types of scams

Invoice scams
This is when scammers pretend to be from a legitimate supplier and attempt to redirect payments for goods/services to their own account. Scammers send an invoice, usually via post or email, requesting payment. They often use company logos and genuine contact details to make communications and invoices look real. The scammers then request payment to a new sort code and account number.

Do not reply to the company through the email thread or the number provided as these can be fake. Before you enter new payment details, check if the bank details are correct by getting in touch with the company via the contact details on their official website. If you have dealt with the company before and have an established relationship with them, you should use these contact details.

Investment scams
You should be cautious of cold callers or emails from investment companies as scammers are trying to tempt businesses to invest their money with offers of high financial returns. They may use a fake website or information brochures that highlight the benefits and include testimonials from fake businesses. Make sure you do your research about the company before committing to anything.

Charity scams
This type of scam is when a person or a group of people pretend they represent a non-existing charity like a local hospital, school or place of worship and seek your help. Scammers try to appeal to businesses' corporate social and community responsibility framework as well as suggesting free media coverage.

Number spoofing
This is when scammers make your caller display show a genuine phone number, for example, your bank or HM Revenue and Customs. This can also happen with text messages.

Useful contacts

If you have been caught out by a scam or you think a friend or family member has been affected, contact Consumerline. They can give advice and, if necessary, pass the matter onto the Trading Standards Service.

For more help and information visit:
www.cyberaware.gov.uk
www.nicybersecuritycentre.gov.uk
www.nidirect.gov.uk/scamwiseni
www.facebook.com/scamwiseni

Consumerline
Tel: 0300 123 6262
Web: www.nidirect.gov.uk/consumerline

Report scams to:

PSNI
Tel: 101 (or 999 in an emergency)
Web: www.psni.police.uk

Action Fraud
Tel: 0300 123 2040
Web: www.actionfraud.police.uk

Reduce unwanted mail and calls by registering with:

Mailing Preference Service
Tel: 0845 703 4599
Web: www.mpsonline.org.uk

Telephone Preference Service
Tel: 0345 070 0707
Web: www.tpsonline.org.uk

This leaflet was produced by The Consumer Council on behalf of the ScamwiseNI partnership.

The Consumer Council
Tel: 0800 121 6022
Web: www.consumercouncil.org.uk

Scams for Businesses

Know the signs... stop the crime

The Consumer Council

scamwiseNI PARTNERSHIP

Communications

Phishing emails and text messages

Phishing emails are used by scammers to get your personal details and the email might even ask you to visit a fake website.

Scammers make the email address and content look like it is from a real company. For example, an official UK Government department offering advice and free financial support.

Never reply to this type of email with information such as your bank sort code, account number or passwords. All official UK Government or public body websites and email addresses end with 'gov.uk' or 'org.uk'. The official National Health Service (NHS) website ends with 'nhs.uk'.

You may also receive text messages offering the same type of advice, free payments, refunds or tax rebates.

Public Wi-Fi

You should never use public Wi-Fi to access your business bank accounts or email as this is less secure than the Wi-Fi in your home or business. Public Wi-Fi is an easy way for scammers to get hold of your confidential information.

If you are in a public place and need internet access, you should use a Virtual Private Network (VPN) or your smart phone as a hotspot.

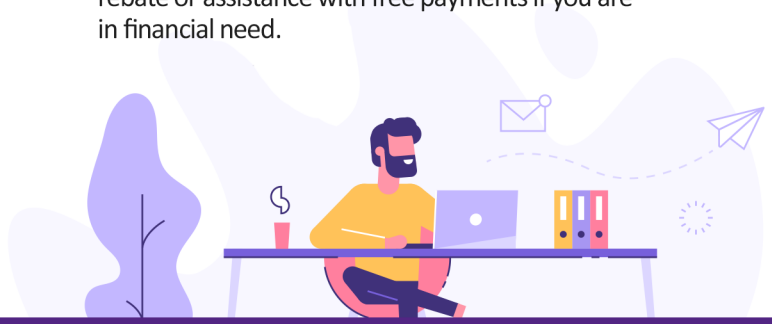
Stay protected

A firewall system and updated software will make sure your computer is protected against viruses and online security threats. Always have strong, unique passwords for each system you use.

It is a good idea to remind your employees of the risk of scams and the different methods scammers use to get personal information.

Top tips

- Contacted out of the blue? Think – is it too good to be true? If in doubt, don't reply. Bin it, delete it or hang up.
- Never send money to a sort code and account number without verifying that the account details you have are correct.
- Your bank will never ask you for your PIN or to transfer money to a 'safe account' because of suspected fraud on your business account.
- Telephone scammers may ask you to call another number like your bank's fraud department but then stay on the line and impersonate your bank to get your details. You should hang up and wait to make sure you have a clear line before dialling the number. Test this by calling a known number such as a friend or family member.
- Keep a copy of your order confirmation and invoice to check against your bank statements to make sure you have been charged the correct amount.
- Never transfer money until you confirm the organisation is real. Just because they sound professional and say they are from the bank, HM Revenue and Customs or a government department does not mean they actually are. These organisations will never contact you by text message, social media or email offering a tax rebate or assistance with free payments if you are in financial need.



Top tips

Top tips for businesses buying and selling goods online

- Be cautious of online marketplaces and social media platforms offering expensive business equipment at low prices. Never make payments to a seller by bank transfer if using these platforms to buy goods.
- When buying goods online you should research the company, read other customer reviews and the description of the item you are buying before making a payment. Some reviews can be fake so always read more than one.
- Before entering your payment details online, check if the web address has 'https' and a padlock icon in the browser bar. This 's' stands for secure and together with the padlock, are important indicators the website is safe but not a guarantee. Do not trust a padlock icon within the web page itself as this can be easily faked.
- Set up the additional security features your bank offers as they give you added protection when buying goods online.
- Take a screenshot or a print out of the goods you are purchasing and the buyer's details in case anything goes wrong.