

# **Business and agricultural scams**

---

Types of scams that are specifically targeted at business owners and agriculture.

# **Types of business and agricultural scams**

## **Invoice scams**

- Scammers pretend to be from a legitimate supplier and attempt to redirect payments for goods/services to their own account.
- They use company logos and genuine contact details to make invoices look real.
- Do not reply to the company through the email thread or the phone number provided as these can be fake
- If this is a company you have dealt with before, you should use these contact details.

## **Phishing emails and text message scams**

- This type of scam is used to get your personal and financial details.
- The email or text message might ask you to visit a fake website.
- Scammers can make the email address look like it is from a real company like an official UK Government department.
- Do not reply to this type of email with information such as your bank sort code or account number.
- Official UK Government or public body websites and email addresses end with 'gov.uk' and 'org.uk'

## **Investment scams**

- Be cautious of cold callers or emails from investment companies.
- Scammers are trying to tempt businesses to invest their money with offers of high financial returns.
- They use fake websites to highlight the benefit and include testimonials from fake businesses.
- Do your research on the company before committing to anything.

## **Phone scams**

- Scammers use number spoofing to make your caller display show a genuine phone number, like your bank. This can also happen with text messages.

- If you are in doubt, hang up and call the company back after a short while using the official details on its website.

## **Charity scams**

- Fraudsters pretend they represent a non-existing charity like a local hospital or place of worship and seek your help.
- They try to appeal to businesses' corporate social responsibility framework
- Do your research on the charity before making a donation. Do not make donations in cash.

## **Online auction/bidding website scams**

- If purchasing items online, the seller may message you and offer additional discount if you pay directly into their bank account.
- Be wary if the starting price is extremely low and not in line with current market prices.
- Never leave the online auction website when asked to make payment.

## **Social media scams**

- Scammers may offer business equipment or supplies at very low prices on social media.
- They are skilled in making photographs of the items look professional.
- If you see an advert offering expensive items at low prices, stop and think – is this too good to be true?

## **Fake online ads selling items for 'free'**

- Fraudsters post ads online for goods that do not exist.
- Avoid sellers online wanting to communicate by email/text message or asking for money upfront.

## **Public Wi-Fi**

- You should not use public Wi-Fi to access your business bank accounts or email as these are less secure than the Wi-Fi in your home or business.
- It is an easy way for scammers to get hold of your confidential information.

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

## **Watch our video about business and agricultural scams**

•

## **Other scams information**

### **How to spot, avoid and report scams**

Information on the different types of scams that you should look out for and how to keep yourself safe.

### **Become a Scamwise Champion**

Inclusive programme to help people with learning difficulties avoid scams.

### **Educational scams activities**

We have developed a range of educational activities that consumers of all ages can get involved in.