# Craft business resource

## Common scams targeting small businesses

Here we summarise some of the most common scams that target small businesses

**Fake invoices**

Fake invoices can look very convincing and may even come from services previously contracted. Scammers can sometimes hijack services' email accounts, which enables them to intercept and edit emails. They can also change addresses on the invoice, paying instructions, and account numbers which allows them to redirect money intended for that service to themselves. Another method is to falsely charge for recurring costs, like renewing a website domain. Always check invoices thoroughly.

**Fake messages**

Since the rise in demand for online shopping, scammers have capitalised on creating fake messages such as missed deliveries. Scammers can track your algorithms when you use your data, whether through your phone, tablet or laptop device, so they can make their messaging appear legitimate. Scammers can hook you in when you reply or click on links provided. Is it Spam or a Scam? Which.co.uk offer advice.

**Unsolicited goods**

A scammer would send a business unsolicited goods and then, having waited long enough for the business either to use or dispose of the goods, send an invoice. These goods are often poor quality, with prices above fair market value. Usually, this scam involves business consumables that are cheap for the scammer to obtain, such as stationery, printer cartridges and cleaning products.

**Fake Directory listings**

Where a business is sent a letter or someone might call asking you to confirm your phone number and address for a print or online directory, the scammer would then invoice for a listing in a directory that may or may not exist. You would then be sent an inflated invoice for the listing. You could also be approached at fairs and events where you might be caught off-guard, so be alert not to sign up to anything without reading all of the small print first.

Supported using public funding by ARTS COUNCIL ENGLAND

**Support publishing and advertising**

In this scam, a rogue publisher approaches a business offering advertising space in a publication associated with a worthy cause, this might include booklets, yearbooks, diaries, calendars or magazines. Sometimes publishers make false claims about their connections with, for example, charities, and sometimes they even mislead these organisations into becoming associated with them.

If the publication is ever printed at all, it is sometimes only in a small print run or with very limited distribution, and there is little or no guarantee that the audience will be relevant or local to the advertiser. If a charity donation is made, it is usually a tiny proportion of the overall revenue.

**Unnecessary services**

When trying to navigate the regulatory requirements for small businesses, scammers often approach with an offer of a paid service to do this work for them. They may mislead businesses into thinking that they are doing so through an official channel or official-looking letters to businesses, making references to legislation and penalties, and demanding information and payment. Sometimes they simply set up websites that businesses can stumble upon when they are looking for the correct, official website to meet their obligations.

The cheapest, and usually easiest, way to meet all these requirements is to deal directly with the body concerned. In many cases, there is no charge at all to notify, register or supply information in accordance with a regulatory requirement.

If you need assistance in completing an official process, you should approach your own advisers, such as your accountant or solicitor. Otherwise, go straight to the official body concerned, such as the Information Commissioner (for data protection registration), the Health and Safety Executive (for health and safety registration) or the Valuation Office Agency (for business rates).

**The phishing/smishing scam**

Phishing is when the scammer sends emails intended to lure you into clicking on a link or downloading an attachment. Clicking or downloading infects your computer with a virus designed to capture your valuable data like passwords, bank accounts, and credit card numbers. Smishing is when the link or download is sent via text.

**Tech support scam**

This would usually start with a pop-up on your computer screen or a phone call from someone claiming to represent a well-known company such as Microsoft. They warn you that your computer is infected and offer to solve your problem at a cost, they will also require remote access to your computer where they can capture your data.

Supported using public funding by Arts Council England.