scam share

spotlight on...

Business Scams

There has been a significant rise in the number of cyber attacks targeting Scottish businesses and people working from home during the pandemic.

what do business scams look like?

The aim of most scam emails is to obtain private business information, login details for business accounts or to persuade a member of staff to transfer money to a scammer's account. Common scams may say:

From: Supplier
We have recently changed our bank account details. Please find attached our new details and your latest invoice for £20,000.

Your Microsoft account password is about to expire. Click on this link to create a new password...

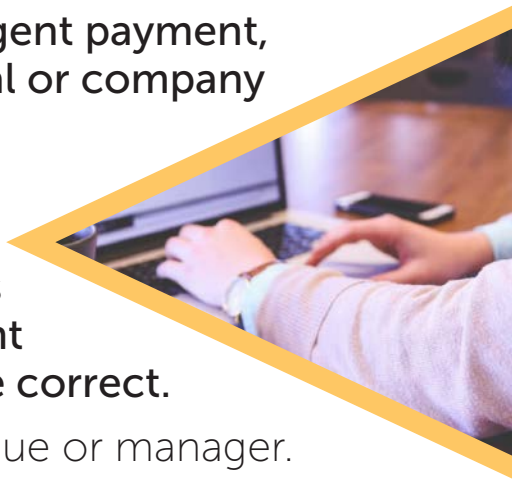
From: IT Department
Click on this link to update your connection to the company network and enter your Office365 login details...

From: Contractor
Our account details have changed - please amend your standing order or direct debit accordingly.

From: Microsoft SharePoint
You have received a file share request - click here to access the following files: 'Staff Reports' and 'Bonuses'...

Trading Standards Scotland

how can I avoid business scams?



Be suspicious of unexpected requests to make an urgent payment, change supplier bank details or provide your personal or company bank details.
Be especially vigilant with changes close to a payment date or changes closely followed by invoices.

Confirm any requests for changes to payment details with the person or company who has supposedly sent them, using contact information that you know to be correct.

If in doubt, get a second opinion from a senior colleague or manager.

Scam emails usually contain spelling mistakes and may not include the company's genuine logo.

Don't click on links in unexpected emails or texts - they may take you a cloned website which will ask for your personal and bank account details.

Question unexpected emails which ask you to log in to an account or click on a link, even if they appear to come from someone within your company.

Check the domain name on any website before entering personal details.

Contact your business's bank immediately if you think you may have made a payment to a scammer or if you are worried that a fraudulent transaction has been made from your account.

If you think that your organisation has fallen victim to a cyber attack, you can call the Scottish Business Resilience Centre's free and confidential **Cyber Incident Response number, 01786 437 472**, for advice and support.

Report all scams to **Advice Direct Scotland** using their free consumer helpline: **0808 164 6000**

If you have lost money or are worried that you have given your bank details to scammers, contact **Police Scotland on 101**.

Find more information and advice on business scams:

Advice Direct Scotland - www.consumeradvice.scot
Police Scotland - www.scotland.police.uk/keep-safe
Scottish Business Resilience Centre - www.sbrcentre.co.uk
National Cyber Security Centre - www.ncsc.gov.uk
Trading Standards Scotland - www.tsscot.co.uk/business-scams

Trading Standards Scotland