FraudSMART.

Informed. Alert. Secure.

Protecting your business from frauds and scams during Covid-19

Businesses are now at increased risk of Covid-19 related scams as fraudsters look to take advantage of the current crisis.

Fraudsters may seek to take advantage of:

- Finance staff and personnel who are working from home.
- Increased and urgent demand for Covid-19 related goods and supplies.
- Increased level of business and payments being done online.

There are two scams in particular that businesses need to watch for:

1. Fake website and fake supplier scams
2. Invoice re-direction scams

Fake supplier/fake website scams and invoice redirection fraud are particularly common right now. Here are the top tips you need to identity these scams and protect your business from falling victim.

Fake Supplier / Website Scams

- There has been a big increase in the number of new website addresses or 'domains' being registered and set up in recent months across Europe.
- The fake domains are fronted by false and malicious websites set up by fake suppliers and vendors who are taking orders for goods and issuing invoices which unsuspecting and legitimate businesses are paying for, but then never receive the goods.
- Europol and their operational partners have warned that over half of new website 'domains' which contain the word 'Covid-19' have been created for criminal purposes.

Banking & Payments Federation Ireland

AIB Bank of Ireland KBC permanent tsb Ulster Bank an post money BARCLAYS

FraudSMART

Informed. Alert. Secure.

Key tips to avoid fake supplier invoice scams

- Only order goods from an authentic/legitimate source – do not click on promotional embedded links in emails, instead use your browser to find your desired supplier and check their official website.
- Thoroughly research any new supplier no matter how big or small your order might be. Check out whether their website has been reviewed online across different trusted sources which aggregate customer reviews.
- Beware of lookalike domain spelling errors in emails and website addresses. Just because an email contains legitimate logos does not mean that it is genuine. Replicated letterheads are also being used.
- Check invoices thoroughly for any irregularities including misspellings and grammatical errors.
- Never issue payment instructions on foot of an email alone. Make additional contact via telephone.
- If you don't know the company or supplier and the offer is too good to be true, it's definitely a scam.
- Consult with your colleagues even when you are working from home.

Invoice Re-direction Fraud

This occurs when a business receives a fraudulent email claiming to be from an existing supplier or creditor advising that bank account details for the payment of future invoices should be changed or made to a different account. The request may not always be accompanied by an invoice, but if the request is acted on it means that any future legitimate payments will be paid directly into the fraudster's account. By the time you realise the money has been paid to a fraudster from a transaction that you authorised on your account, it will have long disappeared.

Key tips to avoid invoice redirection scams

- Pick up the phone to your usual contact in the company (if they are available). If not call someone else in the company to double check the invoice is actually from them.
- Verify all requests purporting to be from your creditors, especially if they are asking you to change their bank details for future invoices.
- Do this by phoning a known contact – do not use the contact details on the letter/email requesting the change. Look up the number independently.
- If possible, set up designated Single Points of Contact with companies to whom you make regular payments.
- Instruct staff responsible for paying invoices to always check them for any irregularities.
- When an invoice is paid send an email to the recipient informing them that payment has been made and to which bank account. Be mindful of account security and consider including the beneficiary bank name and the last four digits of the account to ensure security.
- Fraudsters often look for information regarding contracts and suppliers on an organisation's own website. Consider whether it is necessary to publish information of this type in the public domain and ensure your staff limit what they share about the company on their social media.
- Consult with your colleagues and pick up the phone to them.

If you think your business has fallen victim to fraud or notice any unusual activity on your accounts, contact your bank immediately and report any fraud or attempted fraud to your local Garda station.

FraudSMART is a fraud awareness initiative developed by Banking & Payments Federation Ireland (BPFI) in conjunction with AIB, Bank of Ireland, KBC Bank Ireland, PermanentTSB, Ulster Bank, An Post Money and Barclays.
