

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They have a good knowledge about the organization.

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.



Often, the request is for international payments to banks outside Europe.

The employee transfers funds to an account controlled by the fraudster.

Instructions on how to proceed may be given later, by a third person or via email.

The employee is requested not to follow the regular authorisation procedures.

They refer to an expedited late payment, a need to solve a 'supplier' cash flow issue or the need to procure goods or services urgently.

WHAT ARE THE SIGNS?

- Unsolicited email/phone call
- Direct contact from a senior official you are normally not in contact with
- Request for absolute confidentiality
- Pressure and a sense of urgency
- Unusual request in contradiction with internal procedures
- Threats or unusual flattery/promises of reward

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that **employees are informed and aware too.**

Encourage your staff to **approach payment requests with caution.**


Implement **internal protocols** concerning payments.

Implement a **procedure to verify** the legitimacy of payment requests received by email.

Establish **reporting routines** for managing fraud.

Review information posted on your company website, **restrict information and show caution** with regard to social media.

Upgrade and update technical security.

 Report actual or attempted fraud to Action Fraud or, if in Scotland, Police Scotland on 101.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. **Do not skip any steps and do not give in to pressure.**


Always **carefully check email addresses** when dealing with sensitive information/money transfers.

In case of doubt on a transfer order, **consult a competent colleague.**

Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company's computers.

Restrict information and show caution with regard to social media.

Avoid sharing information on the company's hierarchy, security or procedures.

 If you receive a suspicious email or call, always inform your IT department.

INVESTMENT SCAMS

Common investment scams may include lucrative investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy.

WHAT ARE THE SIGNS?

- You are promised quick returns and assured that the investment is safe.
- The offer is only available for limited time.
- You receive an unsolicited call, repeatedly.
- The offer is only available to you and you are asked not to share it.

A central illustration depicting a financial dashboard with various charts, a world map, and a person on a ladder. To the left, a person in a blue jacket holds a document. To the right, a person in a white shirt stands on a ladder, pointing at a chart. The dashboard features several pie charts, a line graph, and a world map with red location markers. A red circular icon with a white symbol is also visible on the dashboard.

WHAT CAN YOU DO?

- **Always get impartial financial advice** before you hand over any money or make an investment.
- **Reject cold calls** related to investment opportunities.
- **Be suspicious** of offers promising a safe investment, guaranteed returns and large profits.
- **Beware of future scams.** If you have already invested in a scam, fraudsters are likely to target you again or sell your details to other criminals.
- **Report actual or attempted fraud to Action Fraud** or, if in Scotland, **Police Scotland on 101.**

INVOICE/MANDATE FRAUD

HOW DOES IT WORK?

- A business is approached by somebody pretending to represent a supplier/service provider/creditor.
- A combination of approaches can be used: telephone, letter, email, etc.
- The fraudster requests that the bank details for a payment (i.e. bank account payee details) of future invoices be changed. The new account suggested is controlled by the fraudster.



WHAT CAN YOU DO?

Ensure that **employees are informed and aware** of this type of fraud and how to avoid it.

Implement a **procedure to verify** the legitimacy of payment requests.

Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices.

Do not use the contact details on the letter/fax/email requesting the change. Use those **from previous correspondence** instead.

Set up designated Single Points of Contact with companies to whom you make regular payments.

AS A BUSINESS



Instruct staff responsible for paying invoices to **always check them for any irregularities**.

Review information posted on your company website, in particular contracts and suppliers. Ensure your staff limit what they share about the company on their social media.

For payments over a certain threshold, **set up a procedure to confirm** the correct bank account and recipient (e.g. a meeting with the company).

When an invoice is paid, **send an email to inform the recipient**. Include the beneficiary bank name and the last four digits of the account to ensure security.

AS AN EMPLOYEE



Restrict information that you share about your employer on social media.



Report actual or attempted fraud to Action Fraud or, if in Scotland, Police Scotland on 101.

ONLINE SHOPPING SCAMS

Online deals are often a good buy, but beware of scams.



WHAT CAN YOU DO?

- Use **domestic retail websites** when possible – it will be more likely that you can sort out any problems.
- Do your **research** – check reviews before buying.
- Use **credit cards** – you have more chances of getting your money back.
- Pay **only by using a secure payment service** – Are they asking for a money transfer service or a wire transfer? Think twice!
- Pay only when connected to a **secure internet connection** – avoid using free or open public wifi.
- Pay only on a **safe device** – Keep your operating system and security software up to date.
- Beware of ads offering outrageous deals or miracle products – **If it sounds too good to be true, it probably is!**
- A pop-up ad stating you have won a prize? **Think twice**, you might just win malware.
- If the product doesn't arrive, contact the seller. If there is no answer, **contact your bank**.



Report actual or attempted fraud to Action Fraud or, if in Scotland, Police Scotland on 101.

BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

HOW DOES IT WORK?

These emails:

may **look** identical to the types of correspondence that actual banks send.

replicate the logos, layout and tone of real emails.



ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.



Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate.



Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

WHAT CAN YOU DO?

- **Keep your software updated**, including your browser, antivirus and operating system.
- Be especially **vigilant** if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- **Look at the email closely**: compare the address with previous real messages from your bank. Check for **bad spelling and grammar**.
- **Don't reply to a suspicious email**, instead forward it to your bank by typing in the address yourself.
- **Don't click on the link or download the attachment**, instead type the address in your browser.
- When in doubt, **double check** on your bank's website or give the bank a call. If you have lost money to such a scam, report it to Action Fraud or, if in Scotland, Police Scotland on 101.

#CyberScams



ROMANCE SCAM

Scammers target victims on online dating websites, but can also use social media or email to make contact.



WHAT ARE THE SIGNS?



WHAT CAN YOU DO?

- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used elsewhere.
- **Be alert** to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working.
- **Don't share** any compromising material that could be used to blackmail you.
- If you agree to meet in person, **tell family and friends** where you are going.
- **Beware of money requests.** Never send money or give credit card details, online account details, or copies of personal documents.
- **Avoid sending them upfront payments.**
- **Don't transfer money** for someone else: money laundering is a criminal offence.

ARE YOU A VICTIM?

Don't feel embarrassed!
Stop all contact immediately.
If possible, keep all communication, such as the chat messages.
Report actual or attempted fraud to Action Fraud or, if in Scotland, Police Scotland on 101.
Report it to the site where the scammer first approached you.
If you have provided your account details, contact your bank.

BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- **Don't click on links, attachments or images** that you receive in unsolicited text messages without first verifying the sender.
- **Don't be rushed.** Take your time and make the appropriate checks before responding.
- **Never respond to a text message** that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, **contact your bank immediately.** If you have lost money to such a scam, report it to Action Fraud or, if in Scotland, Police Scotland on 101.

SPOOFED BANK WEBSITES

Bank phishing emails usually include links that will take you to a spoofed bank website, where you are requested to divulge your financial and personal information.



WHAT ARE THE SIGNS?

Spoofed bank websites look nearly identical to their legitimate counterparts. Such websites will often feature a pop-up window asking you to enter your bank credentials. Real banks don't use such windows.

These websites usually display:

Urgency: you will not find such messages on legitimate websites.



Pop-up windows: they are commonly used to gather sensitive information from you. Don't click on them and avoid submitting personal data on such windows.

Poor design: be cautious with websites that have flaws in their design or errors in spelling and grammar.

WHAT CAN YOU DO?



Never click on links included in emails leading to your bank's website.



Always type the link manually or use an existing link from your 'favourites' list.



Use a browser that allows you to **block pop-up windows**.



If something important really needs your attention, you will be alerted about it by your bank **when you access your on-line account**.



If you come across a bogus bank website, **report it to your bank**. If you have lost money to such a scam, report it to Action Fraud or, if in Scotland, Police Scotland on 101.

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.



WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank**. If you have lost money to such a scam, report it to Action Fraud or, if in Scotland, Police Scotland on 101.

