

Keep it safe

Helping you protect your
business from fraud



Danske Bank

Making more possible

Peace of mind business banking

We want you to have peace of mind when you bank with us, so ensuring that your accounts are safe is our top priority.

There are also a number of things that you and your colleagues should do to help protect your business from fraudsters.

Please read the following guide and share with your colleagues.

Remember, we will never ask you to:

- reveal codes from your Business eBanking/District eSafeID device. The codes from this device are unique to you, and no-one, not even us, should ever ask for them. The only exception is when you use the services of a Third Party Provider (TPP) through Open Banking and it's authorised by the Financial Conduct Authority or another European regulator;
- provide remote access (or share your screen) to your PC or mobile devices;
- move money to another account for 'security purposes' or in an effort to keep it safe.



Protect your computers and devices

It's important that you take steps to protect your computers and other devices from viruses, malware and other cyber-attacks such as ransomware.

You can do this by:

- installing antivirus software and a firewall. We provide Webroot Secure Anywhere® free to all our Business eBanking/District customers. Further information is available when you log on to Business eBanking/District.
- running a full virus scan of your workstation monthly, and ensuring your antivirus system checks for updates weekly.
- installing all recommended operating system and program updates to help protect against any known system and software vulnerabilities. You can easily set updates to run automatically.
- ensuring that you only download files or programs from the internet where you have a specific reason and if they're from **genuine, trusted websites** or senders. If you receive a Microsoft Office document attachment from a trusted sender, you should always open it in 'Protected view'.
- creating **strong passwords** using a combination of letters, numbers and special characters. Avoid using common words or personal details. You should update your passwords regularly and use different passwords for different systems. For example, your password for emails should not be the same as your Business eBanking/District password.

Use our business online banking security features

While we work hard to protect you whilst using Business eBanking/District, our online banking platform, there are a number of things that you should also do.

We recommend:

- you regularly review all user authorisations and remove a user when they are on extended leave or leave the business permanently. An Administrator can delete or block a user immediately.
- setting up dual authorisation so that payments initiated and approved by one user require authorisation by a second user before they take effect, making it more difficult for hackers to make payments in your name.
- when using dual authorisation, each user logs on from a different computer or device. For example, one user could create and authorise the payment on a PC or Laptop and a second user complete the second authorisation on our Mobile Bank App. Danske Bank will **never issue a pop up** requesting a second user to log on to the same device to complete a payment authorisation. If you see a prompt like this, you should discontinue your use of Business eBanking/District and contact us immediately.
- using **payment limits** within the Administration module in Business eBanking/District to create a payment limit on an account and/or on an individual user, depending on your requirements.
- locking your **creditor listing** so that payments can only be made to a regular list of creditors or choose who can set up and approve a new creditor.

Keep it safe

Remember you're responsible for keeping your personal User ID, password and numbers from your eSafeID safe.



You should **never share** your password or codes from your eSafeID device with anyone (including the Bank) and each Business eBanking/District user should have their own User ID.

Be vigilant



While fraudsters are continually evolving their methods, there are a number of common scams that you should be aware of:

- **Invoice redirection/Mandate Fraud**
Watch out for fraudulent emails or text messages claiming to be from a supplier, advising of a change in bank account details. Don't reply to the message, instead check directly with the supplier or person requesting the change, to ensure it is a genuine request before you transfer money. The same advice applies for payments to new beneficiaries/suppliers.
- **CEO fraud**
Be particularly cautious if you receive an email or a text message from a colleague, manager or CEO asking you to transfer money. Always check directly with the person that it is a genuine request.
- **Malware**
Be wary of unexpected emails and text messages that appear to be from banks or other reputable companies asking you to click on links, download attachments or share personal information.
- **Telephone call from phone or software company**
A genuine company is very unlikely to contact you and ask you to download third party software or request remote access to your device. If in doubt, end the call immediately and call the company back on a recognised phone number (ideally from another phone line).

Suspect fraud?

If you suspect fraud, an unauthorised transaction or misuse of Business eBanking/District, contact us immediately on our 24 hour telephone service:

UK number	International number
0800 917 7918	0044 800 917 7918

More information

To find out about different types of fraud and get more advice on keeping your business accounts safe, visit danskebank.co.uk/security.

This publication is also available in Braille, in large print, on tape and on disk. Speak to a member of staff for details.

Danske Bank is a trading name of Northern Bank Limited, which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, Financial Services Register reference number 122261.

Registered in Northern Ireland R568.

Registered office:

Donegall Square West

Belfast BT1 6JS

Northern Bank Limited is a member of the Danske Bank Group.

danskebank.co.uk

