Keep it safe

Helping you protect your business from fraud

danskebank.co.uk

Danske Bank

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.

Be vigilant

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

- **Invoice redirection or beneficiary account change fraud**

  Watch out for 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 (either in person or by the phone) 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.

  Criminals can also amend the bank details on invoices. We recommend that you verbally confirm (either in person or by the phone) the accuracy of the beneficiary details with the intended recipient before sending any payments.

- **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 or purchase gift cards. Always check directly with the person (either in person or by phone) that it is a genuine request.

- **Malware and Ransomware**

  Be wary of unexpected emails and text messages asking you to click on links, download attachments or share personal information.

- **Impersonation scams**

  Phone calls from criminals pretending to be your bank, the police, a phone or software company, a government department (e.g. HMRC) or any other well-established company.

  A genuine company is very unlikely to contact you out of the blue and ask you to transfer money (for instance to a 'safe account'), to download third party software or to request remote access to your device. If in doubt, end the call immediately and call the company back on a phone number you know to be correct (ideally from another phone line).

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 District customers. Further information is available when you log on to 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 District password.
- Further protect access by enabling **two-factor authentication** on systems including emails. Please refer to your IT security support for more information.

Use our District security features

While we work hard to protect you, there are a number of things that you should also do. We recommend:

- you regularly check your current **District Users** and their authorisations to make sure they're still suitable for your business. See our guide, 'Viewing User Authorisations' at danskebank.co.uk/busdocs for help.
- setting up **dual authorisation** so that payments initiated and approved by one user require authorisation by a second user before they debit your account. This makes 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 District and contact us immediately.
- using **payment limits** within the Administration module in 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 details with anyone (including the Bank) and each Business eBanking/District user should have their own User ID.

Remember, we will never ask you to:

- share the one-time passcodes that we text you or those from your eSafeID device. These codes are unique to you; 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;
- install programs on your computer or request remote access to your devices or screens;
- move money to another account for 'security purposes' or in an effort to keep it safe.

Suspect fraud?

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

UK number: 0800 917 7918
International number: 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.

We may record or monitor calls to confirm details of our conversations, and for training and quality purposes.

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

danskebank.co.uk

Correct as at 09/2022

10014UK