

A reminder about the importance of online security



Here are our Top IT Security Tips which you should be familiar with:

- **Make sure you install antivirus software.** You should choose software that scans for viruses and ensure that you update the program regularly to keep continual protection against new viruses. Set up your antivirus program to automatically check for viruses when you download files from the internet.
- **Keep your operating software up to date** with patches, firewalls etc. and set your internet browser to the highest level of security.
- **Be cautious about opening unsolicited emails.** If you do not know the sender or receive an unexpected email, you should consider deleting the email without opening it first. Be particularly cautious about opening emails with attached files, as well as emails with odd names or emails in another language.
- **Never follow links to our Business eBanking system from an email.** Instead you should always type our website address into your address bar.
- The 'http' at the beginning of our website address will always change to 'https' when a secure connection is made and remain throughout the connection. Be wary of unexpected or suspicious 'pop ups' during your Business eBanking session.
- When you log on to Business eBanking your **Password will never be shown** on screen – instead you will see a series of dots. If your password is visible on screen you should contact Customer Support immediately.
- **Think carefully before giving out personal information** on the internet, by email or by phone. Only send encrypted confidential information and only to people you know. In particular, never divulge usernames, passwords and eSafelD device numbers to anyone - not even if that person states that they are a Danske Bank employee.
- **Never leave your computer unattended** when you are logged into Business eBanking.
- Make sure you **log off Business eBanking as soon as you are finished.**
- **Only download programs from known and credible websites.** Never open programs directly. Instead, save them on your hard drive and have your antivirus software check them before you open them.
- **Use our Administration module** to select which accounts your users have access to, to set individual user payment limits - by monetary amount in a specified period, or to restrict user access to creating and authorising payments only to a locked list of beneficiaries.
- If you do not have joint authorisation for payments already, **you should consider changing your payment authorities to require two electronic signatures.** This creates additional security for your business and is our recommended solution for authorising online payments.

Remember: a Danske Bank employee will NEVER contact you by any means, and ask for your Business eBanking log-on details.

You can view further tips and advice on our website at danskebank.co.uk/security

If, at any time, you think that the security of your Business eBanking has been compromised, please call our Customer Support team immediately on **028 9031 1377**.

Customer Support's business hours

Monday to Thursday*	8.00 - 20.00	Friday*	8.00 - 17.00
Saturday*	9.00 - 17.00	Sunday*	9.00 - 20.00

* except for bank holidays or other holidays in Northern Ireland when the bank is not open for business. We may record or monitor calls for your protection, to train our staff and to maintain the quality of our service.

Call charges may vary. Please refer to your phone company for more details.

Business eBanking may be temporarily unavailable when we are carrying out routine maintenance.

Danske Bank