11572.0314

Info@sydbank.dk
sydbank.dk

Sydbank

Useful advice – using the internet securely

Sydbank

Using the internet securely

By observing a few basic rules when surfing the internet or receiving emails, you can do a lot to protect your computer from intrusion, viruses and other malicious attacks.

Therefore please read the following security tips before using Online Banking/NetBank:

1. Never click on a link or open an email attachment if you are unsure about its contents. Be particularly suspicious of all unsolicited emails and emails from unknown senders. Be extra careful when unsolicited emails contain links and attachments – do not click on them.

   The same applies to phishing emails in which you are requested to disclose personal data. Often such emails claim to have been sent from for instance a bank, Nets, the Central Customs and Tax Administration or Visa. In many cases they contain a link – but if you click on it you enable hacker attacks against your computer. Delete phishing emails and do not click on attachments or links.

2. Always keep your browser, email client, utility software and operating system updated to the most recent versions so that you always have the latest security updates.

3. Always use updated anti-virus software which automatically scans files, email attachments etc, before they are stored on your computer.

4. When communicating securely over the internet you will see a padlock icon at the top or in the bottom right-hand corner of your browser. Click on the padlock icon to verify with whom you are communicating.

5. Make sure that your company's IT equipment and network are protected by an updated firewall.

6. Set your browser to alert you before anything is downloaded to your PC. Only allow downloads from sites/sources you are familiar with and trust. Check the certificate – see 4.

7. Choose a password which is difficult for others to guess and keep it secret/personal. Change your password at regular intervals.

8. If you use a wireless network, remember to enable encryption. If necessary, contact your IT supplier or telecommunications provider.

9. Only use Online Banking/NetBank on computers which you control. And remember to always log out correctly.

10. If others have remote desk access to your network such access should be restricted to the widest extent possible with IP address and password approval.

The latest information is available on the Online Banking/NetBank login page.

Who covers misuse of Online Banking/NetBank accounts?

If Online Banking or your NetBank has been broken into by IT criminals, different rules apply as to who is liable for any resulting loss, depending on account type (retail account or corporate account).

Retail accounts

If retail accounts have been misused and the user has taken ordinary precautions, the Bank will cover any loss as a rule.

Retail accounts used to make corporate payments are considered as corporate accounts.

Corporate accounts

Corporate accounts are not covered in the same way as retail accounts. Consequently the company itself must cover any loss resulting from break-ins into corporate accounts.

Protect yourself from losses resulting from misuse of corporate accounts

Even though the company has clear business procedures to secure its IT systems, break-ins may occur, for instance if an employee opens an infected email, website or downloads a program that contains spyware or similar. We recommend that you take out insurance against loss resulting from unauthorised use.
Contact your insurance company or your auditor for more information.

If you suspect ...

If you have clicked on a suspicious email or if you suspect that your PC has been infected with a virus, you must avoid logging in to Online Banking/NetBank and contact Sydbank's Hotline immediately to block Online Banking/NetBank. Sydbank Online Banking users must call Sydbank's Hotline on +45 74 37 25 10.
Sydbank NetBank users must call Sydbank's Hotline on +45 74 37 25 98.
Outside our business hours, please contact Spærreservice (block service) on +45 75 94 50 93.