MitID Security Guide

You prove who you are when you log on and authenticate with your MitID, and it is important that you protect your MitID.

If you follow the recommendations below, your MitID will be more secure:

Your MitID is yours and only yours

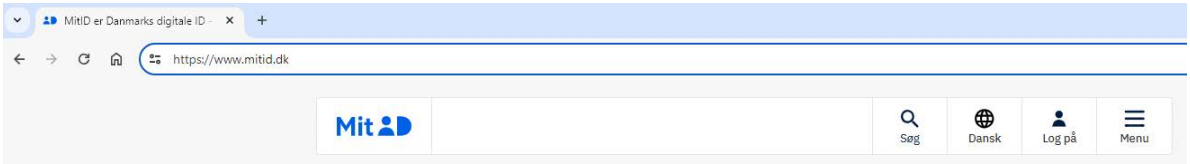
Do NOT share your MitID or your MitID information with others. Your user ID and your codes are private, and when they are safe your identity is safe.

Don't ever click on links in SMS or emails

A link can take you to a different place than where you think you are going.

The most common type of fraud on the internet are when users click on links that takes them to fraudulent websites. The site looks right but it isn't. When you attempt to log on to a false website, you are giving your logon information to the criminals behind the website.

To avoid being cheated this way, you can type in the web address yourself when using a browser like Firefox, Chrome or Safari – like writing www.mitid.dk – in the address bar. If you write the address yourself, you will get to the correct page.



Make it a habit to check the web site's address in the address bar.

- Examples of genuine addresses: www.mitid.dk, yourbank.dk
- Examples of false addresses: mitid.dk.bank.com or mitid.com/mitid.dk

If you are in doubt whether an address or a homepage are genuine, always contact MitID support.

Don't ever provide information over the phone

If you receive a phone call soliciting your MitID information, it will be a fraudulent attempt to get your information.

Scammers, who contact you by phone, can be very convincing. If you have the slightest suspicion, please follow this advice: Hang up and contact MitID support on the phone number you find on www.mitid.dk.

Don't ever call a phone number that the scammers have given you, even if it sounds legitimate. Only use the phone number you find on www.mitid.dk.

Security guide for MitID authenticators

It is important that you protect your MitID authenticator against theft and abuse.

We recommend that you create and activate more than one authenticator for your MitID user. If you install the app on your smartphone and your tablet, you will be able to access and activate your MitID on a new smartphone, should your old one be missing.

MitID app

We recommend that you use the MitID app downloaded from Google Play or Apple App Store.

You can have MitID installed on three devices but remember the following:

Only install the MitID app on the smartphone or tablet that you control. It could be your private smartphone, your work phone, and the family tablet.

Remember to protect your PIN code for MitID app. Don't ever write the PIN code on anything, don't tell it to others, and don't use the same code to open your MitID app that you use to open your smartphone or tablet.

The MitID app is secure because:

- The MitID app clearly displays what you are about to authenticate and where. This could be when you are transferring money using your online bank or logging on to a specific site.
- MitID app has a 6-digit PIN code. You can also choose to use fingerprint or facial recognition for access.

MitID code display or MitID audio code reader

Be as protective and secure with your MitID code display and your MitID audio code reader, as you are with your house keys. We recommend that you attach your MitID code display to your keychain and carry it with you. The MitID audio code reader doesn't fit on your keychain.

If you use MitID code display or MitID audio code reader, you must remember to:

- Don't ever hand over the MitID code display or the MitID audio code reader to another person.
- Don't ever share your MitID code reader's one-time password code with others regardless of who they are. Do not send one-time password codes to others using chat, SMS, or email.
- Only enter one-time password codes from your MitID code display or your MitID audio code reader, when you log on or authenticate with MitID.
- When you enter one-time password codes from your MitID code display and your MitID audio code reader, you will follow a fixed process that you will learn to recognize. If you encounter any deviation from this process – something that appears different from the normal process – please close your browser immediately and contact MitID support.

MitID chip

You should be as careful with your MidID chip, as you are with your house keys. We recommend that you attach your MitID chip to your keychain and carry it with you.

If you use MitID chip, you must remember:

- Never hand the MitID chip over to another person.
- Be extra careful the first time you connect your MitID chip to your computer, smartphone or tablet. Make sure that you are in a safe place that prevents others from intercepting your data, when you make the connection. A safe place could be in your home or at your job.

Passwords for MitID

If you are using the MitID code display, the MitID audio code reader or the MitID chip, you must create a MitID password that you will use, when you log on or authenticate using MitID. Here are some recommendations on how to create a safe and secure password.

Only use your MitID password with MitID

A password is unique and should be used only to provide specific access to only one website, despite the common practice to share password between sites. If scammers obtain your password from one website, they might use it to log on to other sites and pretend to be you.

Create a strong password

Your MitID password must contain at least 8 characters. To create a strong and secure password follow these steps:

1. Choose a “strong” word that you can remember.
2. Use each letter from the “strong” word as the first letter in a new word and put the new words together in a sentence in the order that spelled the “strong” word.
3. End the sentence with a number.

Examples of strong words and passwords:

- Strong word “BOARD” can create the password *BingoOwlAnchorRainDoor5*
- Strong word “HOUSE” can create the password *HintOwlUtilitySingerEnd7*
- Strong word “CAR” can create the password *CalenderAnchorRailway1*

Create your own “strong” word and password.

Don’t ever write your password on anything

If you fear that you will forget your password, we recommend that you use a Password Manager to help you manage your passwords.