

# Using Megabank securely

Bank Mendes Gans  
Version 3

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Updates and disclaimer	3
<b>2</b>	<b>Making sure you're really on Megabank</b>	<b>3</b>
<b>3</b>	<b>Protecting your scanner, credentials and devices</b>	<b>3</b>
3.1	What can you do to protect your credentials and devices?	4
<b>4</b>	<b>If you lose your scanner or a device holding the Megabank app</b>	<b>4</b>
<b>5</b>	<b>Protecting yourself against phishing and malware</b>	<b>5</b>
5.1	Phishing emails and spoof websites	5
5.2	Malware	5
5.3	What can you do against phishing and malware?	5
5.4	What to do if you recognize phishing or malware	6
5.5	Safely granting permissions to other users	6
<b>6</b>	<b>Protecting yourself against CxO fraud</b>	<b>6</b>
6.1	What can you do against CxO fraud?	6
<b>7</b>	<b>Protecting yourself against invoice fraud</b>	<b>6</b>
7.1	What can you do against invoice fraud?	7
<b>8</b>	<b>Contact details for reporting fraud immediately</b>	<b>7</b>
8.1	If your BMG contact is not available	7

## 1 Introduction

You can use Megabank with confidence because we use up-to-date technologies and firm policies for secure authentication and data protection. We treat all information you share with us with the strictest confidentiality. You are the only one who has access to your account. To safeguard the security and integrity of our business, we log and monitor your activity on Megabank.

In this document, we'll talk about the measures you can take to protect your logon details and devices, how to protect yourself from common types of fraud, and what to do in case something goes wrong. Don't hesitate to contact your account manager if you have any questions.


### 1.1 Updates and disclaimer

We may modify this security message without prior notice to reflect recent developments and new insights. Please check this security message from time to time for any changes.

The information in this message is provided to you solely for informational purposes: to make you aware of the most frequent cases of fraud and provide you with recommendations to protect yourself against it. This information does not ensure that your company, acting upon these recommendations, is or will be protected against any occurrence of these types of fraud. You cannot derive any rights from the use of and reliance on the safeguards you take by following up these recommendations. BMG does not accept any responsibility or liability with respect to your reliance on and the actions you take as a result of these recommendations.

## 2 Making sure you're really on Megabank

The use of internet for banking services implies the risk of cybercrime. So please be careful and take adequate security measures. When logging on to Megabank, always check four things carefully:

1. there must be a padlock symbol in the address bar of your web browser, just before the URL: 
2. the address must start with **https://**
3. the domain name must read **www.megabank.nl**
4. click the padlock symbol to check if the security certificate is valid and owned by 'Bank Mendes Gans [NL]'.

## 3 Protecting your scanner, credentials and devices

Your app and mobile PIN or scanner and PIN are the keys to your account. Protecting these and your computer or mobile device is your responsibility. Except for logging on to Megabank, BMG will never ask you for your logon credentials. So be very suspicious if you are asked to provide your logon credentials in an email or a phone call. Never write your PIN or mobile PIN down, and never give it to anyone else or include it in an email.

Note that a mobile device that has the Megabank app installed functions as a scanner – making it extra important not to allow other people access to that device.

### 3.1 What can you do to protect your credentials and devices?

- > Prevent unauthorized people from using your computer or mobile device.
- > Don't use unsafe computers, for example in an internet cafe or hotel.
- > Don't install the Megabank app on unsafe mobile devices. This includes devices that have been 'rooted' or 'jailbroken' to bypass their factory-set limitations.
- > Log off or lock your workstation every time you leave your desk.
- > Protect your mobile device and the Megabank app with biometric access, like facial or fingerprint recognition. Make sure only *your* facial profile or fingerprints are stored on your device.
- > Make sure your computer and mobile device are protected by anti-virus software and firewalls.
- > Use operating systems and other software from reliable vendors only. And keep this software up to date on all your devices.
- > If possible, get the Megabank app from the Apple's App Store or Google Play. If you don't want to or can't use Google Play, download the Megabank app from [www.megabank.nl](http://www.megabank.nl) and install it on your Android device. To do so, you'll have to allow your phone to install apps from external or unknown sources. We recommend you disallow this again as soon as the Megabank installation is complete.
- > Allow your operating systems and the Megabank app to update automatically. That way you always receive the latest security updates immediately.
- > Always be careful sharing files when connected to a network, especially with open connections such as Wi-Fi. Turn off your file sharing options or apply very strict settings.
- > Change your passwords often and choose passwords that are hard to guess.

## 4 If you lose your scanner or a device holding the Megabank app

If your scanner gets lost or has been stolen, or if you notice any improper, unauthorized or fraudulent access or use of your Megabank account, report the incident to your coordinator immediately. Check 'Your contact at your company' on Megabank. He or she will block your scanner or account and determine the follow-up actions.

If you lose the device that holds your Megabank mobile app, just activate the Megabank app on another device to secure your Megabank account. Your partner's device, for example, or your colleague's. The reason is simple: each Megabank user can only have one device with a functional Megabank app. So activating the Megabank app on a new device automatically renders it useless on your old device: as soon as you log onto the Megabank app on the new device, you're in control again.

Once you have installed Megabank on a borrowed device after losing your own, you can simply deactivate it before you return the device to its owner:

- > Log onto the app with your PIN.
- > Tap the hamburger menu on the lower right.

- > Tap 'Settings'.
  - > Under 'Account', tap 'Unregister' and confirm with 'Yes'.
- This way, you're a hundred percent sure there are no devices in circulation with a Megabank app that's linked to your user account.

If you don't (immediately) have access to another device on which to install and activate the Megabank app, just call or email your coordinator: they'll block your user account temporarily. Whenever you are ready to install Megabank on another device, ask your coordinator to unblock your account. As soon as your user account is unblocked, you can install and activate the Megabank app on a new device.

Whether you've lost your scanner or your mobile device: in all cases the alternative is to contact your BMG service team.

## 5 Protecting yourself against phishing and malware

Phishing and malware infections are common ways to commit e-banking fraud that you can encounter both privately and professionally. Cyber criminals will try to steal money by obtaining identification codes and electronic signatures of their victim. With these codes, they transfer funds to their bank accounts by emptying yours.

### 5.1 Phishing emails and spoof websites

Criminals create authentic-looking, but false or 'spoof' websites. Their purpose is to trick you into giving up your personal information, such as your user ID or other security credentials. They will then use this information to gain access to your account. Fraudsters increasingly turn to email to generate traffic to their spoof websites. This practice is known as 'phishing'.

BMG will never send you an email asking for any confidential or personal information. If you ever get an unsolicited email with an embedded link, or a request for personal details, do not click the link or respond in any way, but forward the email as an attachment to [phishing@mendesgans.nl](mailto:phishing@mendesgans.nl). In Outlook: use the key combination Ctrl+Alt+F.

### 5.2 Malware

Please be aware of malicious software or 'malware'. There are many ways in which criminals will try to target your computer or mobile device by installing malware, that will capture your personal data and redirect you to spoof websites. We advise you to always keep your antivirus and other software up to date on all your devices.

### 5.3 What can you do against phishing and malware?

- > Install anti-virus software and keep it updated. If you are unsure how to do this, read the program's Help function or contact your company's helpdesk.
- > Use spyware removal software and keep it updated. If you are unsure how to do this, read the program's Help function or contact your company's helpdesk.
- > Install firewall software: firewall software protects your computer and its contents from criminals. Its aim is to prevent unauthorized traffic to and from your computer.
- > Check that you log onto the correct page: <https://www.megabank.nl/>.

- > Check the padlock symbol in the address bar of your browser. That means that the connection is secure.
- > And check whether the certificate has been granted to 'Bank Mendes Gans [NL]'.
- > Always double-check the details, i.e. amount, beneficiary name and account numbers of all payments you are about to sign.

#### 5.4 What to do if you recognize phishing or malware

- > If, at any point, you fear that your computer or mobile device has been successfully targeted, contact your company's helpdesk as soon as possible to take all necessary measures to prevent any loss or damage.
- > If, at any point, you are concerned you may have disclosed your security details, or if you find a spoof of our website, please contact your account manager at BMG immediately.
- > If you think the incident might jeopardize Megabank's integrity, please contact your account manager at BMG immediately.

#### 5.5 Safely granting permissions to other users

If you can grant and upgrade Megabank authorizations to other users, try keeping the initiative on your side. When a user does reach out to you requesting (more) authorizations, make sure to confirm their identity in person or by phone. This way you prevent unauthorized parties from fraudulently obtaining Megabank permissions.

## 6 Protecting yourself against CxO fraud

CxO fraud is a form of social engineering: manipulating people so that they disclose confidential or sensitive information. A fraudster poses as a senior manager (someone of the C-suite, hence 'CxO Fraud') to manipulate employees into executing payment transactions or divulging confidential information.

#### 6.1 What can you do against CxO fraud?

- > Always act cautious when funds are asked to be transferred urgently and secretly.
- > In the event of an urgent request, always call the person who made the request back on a known, previously verified phone number.
- > Implement segregation of duties like dual signing permissions, where at least two separate people have to sign payments. Also make sure that signing is always done properly, following company's protocol, not just sign off based on trust.
- > Never share your scanner or your PIN.
- > Limit the level of detail in your social media expressions on the role you occupy within your organization.

## 7 Protecting yourself against invoice fraud

Invoice fraud comes in many forms. In all cases, the fraudsters will change the banking details of the company that issued the invoice to their own, and as a result, receive the invoiced amounts. It doesn't have to involve intercepting and modifying invoices: it can be as simple as a fake email that seems to be sent by a supplier, stating a change of bank and consequently of account number. This message will

bear the supplier's letterhead and seem legitimate; if the recipient follows the instructions, all pending and subsequent invoices will be paid to the new – fraudulent – account number.

### 7.1 What can you do against invoice fraud?

- > Validate invoices: check whether you expected an invoice for this amount and check if the supplier details are unchanged compared to previous payments.
- > Inform your customers that if they receive a request to change your details (address, phone number, email address, account number, etc.), they should call you on a previously verified phone number to check if the requested change is valid. Your customers shouldn't use any unknown phone number indicated on the request itself.
- > The same applies to you: if you receive a request to change your supplier's details, make a phone call to a previously verified number to check the validity of the requested change. Again, don't use any unknown number indicated on the request itself.

## 8 Contact details for reporting fraud immediately

If fraud has been detected and it's still in progress, notify your BMG contact right away. Even if a transfer has already been made, we can try to retrieve or block the funds before they disappear permanently from the beneficiary account. Speed is of the essence, because the chance of reversing your transaction diminishes with every passing minute.

### 8.1 If your BMG contact is not available

If you can't reach your BMG contact, please **call ING Wholesale Banking, Fraud Operations at +31 20 584 7840**.

- > An ING employee will answer your call.
- > Emphasize that you are a customer of Bank Mendes Gans, and that a fraudulent transaction is in progress that needs to be recalled. Provide as much information as possible (e.g. account number, amount, currency, beneficiary account, description and date).

Fraud Operations is available at the following times:

- > Monday to Friday: from 07:00 to 00:00 Amsterdam time
- > Saturday: from 08:00 to 17:00 Amsterdam time
- > Sunday: closed

After working hours or for a fraud that occurred in the past, please contact [fraudpayments@ing.com](mailto:fraudpayments@ing.com).

## Contact

**Author**

Bank Mendes Gans

**Version**

3

**Email**

[info@mendesgans.nl](mailto:info@mendesgans.nl)

**Internet**

[www.mendesgans.nl](http://www.mendesgans.nl)

**Bank Mendes Gans**

Herengracht 619  
1017 CE Amsterdam  
The Netherlands