bunq

BANK OF THE FREE

Safe Banking

bunq

1. Welcome

This document is here to provide you with some insights on how to keep your banking experience safe and secure. We will explain to you what the common types of fraud are and how to recognise them.

2. Common types of fraud

Phishing

What is phishing? Phishing is an attempt by fraudsters to obtain your personal information such as passwords or security details. A fraudster often disguises themselves as a trustworthy party by using fake websites. The appearance as well as the webpage link are often almost exactly the same as the original website. These fake pages are very good at making you believe they are sending a genuine email from (for example) your bank or an online payment processor, when in fact it is fake.

If you receive an email or other messages that resembles bunq's normal messages, in which you are asked to follow a link and log in, or share your login codes or other security information, please do not follow these instructions.

bunq will never ask you for your login codes or security features either by phone (we don't use phone calls as a way of communication), via e-mail, text message, WhatsApp or any form of social media.

If you do not trust a website or are unsure about the validity of the website, you can always check when the website was registered. If it was registered recently, this might indicate that it is fraudulent.

bunq

Do you want to know more about phishing? Read all about it on www.bunq.com/phishing-scams.

Old-fashioned phishing

This happens when you are entering your PIN at an ATM or at a payment station. Please make sure that no one is watching you and that you always cover your PIN whilst you are entering it.

Always store your card safely.

Spoofing

Spoofing means disguising an unknown sender as a trusted and known sender.

What may happen is that fraudsters:

- send emails that seem to be sent from a trusted address (e.g. your bank or other trusted institutes);
- send you texts that seem to be sent from a trusted number;
- call you from a phone-number that shows as your banks' phone-number.

These kinds of fraud are known as "spoofing" or help-desk fraud. How do you recognise it? Fraudsters may ask you to confirm your log-in details, or tell you that there has been some strange activities on your account and ask you to transfer your money to a "safe-keeping account". Banks, however, will never ask you to give up your log-in details, and will never ask you to transfer money to another account

bunq

WhatsApp fraud

WhatsApp fraud is a form of fraud where someone pretends to be someone you know and asks you to help them out with the payment of a bill through a WhatsApp message. Usually, the following characteristics apply:

- The person has a new number and contacts you through WhatsApp.
- They ask you for help by paying a bill for them.
- They are in a rush, the bill needs to be paid quickly.
- They cannot, or do not want to communicate with you through any other means than WhatsApp.

If anyone asks you to transfer money or pay an existing bill for them, contact this person through other means of communication outside of WhatsApp. When you cannot reach this person, do not transfer any money.

How can you help stop this kind of fraud? If a payment link was provided by the scammer, make sure to report this and/or the IBAN to the police and us.

Fake payment requests

If you receive a payment request, always check the validity of the web page the link leads you to (especially from someone you do not know). Often fraudsters will use fake internet pages which look very similar to the normal payment environment of your bank.

The information you enter in this website is directly visible to the fraudsters and may be used to access your bank account.

Never enter your bank account information if you do not trust the payment link or the person that is sending you the payment request.

bunq

Marketplace fraud

You may stumble across a bargain on a second hand website. Great! Along with saving money, you will also contribute to a greener planet. Unfortunately, the person who promises to send you the product doesn't always fulfil the order and deliver the item after you have paid.

In addition, it is quite common for fraudsters to trick you into sending fake payment requests; the 'so called' €00,01 cent payments, because they want to "check that you are a real person, and not a scammer". These payment requests are often fake.

How do you recognise these fraudsters? If something sounds too good to be true, this is usually because it isn't true. Always check the market value of the product you want to purchase. If the price that is offered to you is much lower, this can be a sign that there's a fraudster at work!

Also, we'd recommend researching the website you're using to check if there are any red flags or warnings about possible fraud.

Do NOT become a money mule!

If anyone reaches out to you to ask for access to your bank account or to transfer some money through your bank account, **never comply with this request**, no matter how promising the reward may sound.

Here's an example: someone reaches out to you through social media and promises to give you money. In exchange for this, they need to use your existing bank account, or they ask you to transfer some money for them. They tell you it is only for a (few) day(s), and they reassure you that there's no risk involved and that it's really easy to earn some money this way.

bunq

It is highly likely that your bank account will be used by these people for illegal activities, for which you will be held (criminally) liable. It is your bank account, so you are the one who's name is connected to this criminal activity!

Consequences of you being held liable, may be that you will not be able to open any bank accounts anymore, get a mortgage or obtain credit and that criminal proceedings may follow!

Again, please realise that if something sounds too good to be true, this is because it isn't true!

If someone in your circle is involved with this kind of activity, please warn somebody close to this person to have a talk with them.

For more information on money mules, check out this post by the Dutch police by going to www.politie.nl/nieuws/2020/oktober/7/03-word-geen-geldezel.html.