In response to a security incident that recently occurred involving the email box of one of the civil-law notaries, we listed below a number of frequently asked questions and our response to them.

If after reading the responses you still have some questions, please send them to the following email address: incident-response@owknotarissen.nl.

Questions and answers

What happened?

On 19 October 2021 we discovered that a hacker had successfully gained access to the email box of one of our civil-law notaries, and probably also to the data in that mailbox.

Following this security breach, a number of contact persons received Phishing mails, asking them to click on a link. It is clear from this that email addresses had been accessed.

We cannot rule out that the hack also involves the attachments in the emails which you and we have sent. These could also be copies of identity documents and/or deeds and draft deeds.

Which email box has been hacked?

For security reasons, we are not giving those details on this website. We informed the persons concerned once we had established who had had contact with this mailbox.

What can a hacker do with these data and what are the potential consequences and risks?

The data have been used to send Phishing mails, in which the hacker poses as a civil-law notary or an employee of our firm with the aim of getting the recipient to click on a link. It cannot be ruled out that a hacker could also commit identity fraud.

The government has explained the potential consequences of this at

https://veiliginternetten.nl/maakhetzeniettemakkelijk/.

https://veiliginternetten.nl/thema/basisbeveiliging/wat-is-identiteitsfraude/

You must be alert to any emails you receive that ask you to act quickly, transfer money or click on links that take you to a fake login page, or warn you about non-existent threats such as viruses or ‘suspicious activities’ in your bank account, after which you are asked to transfer your funds to a ‘secure account’. This is standard Phishing mail behaviour, but since it is linked to an existing contact, the mail may appear to be slightly more genuine and urgent.

In an exceptional case, documents sent may be referred to or the personal data breached may be misused.

If you come across this, please would you contact us.

The investigation into a breach involving the attachments is still ongoing, and as soon as we can establish that this has not been part of the hack we will inform all those involved.

What can I do if I am approached by a hacker via email?

You should delete this suspicious email immediately, and definitely do **not** click on the link.

You can often recognize such an email if it comes from an unfamiliar source (email address).

The emails that our firm sends always contain the suffix: **@owknotarissen.nl.**

Please also follow the government recommendations given on this site: https://veiliginternetten.nl/maakhetzeniettemakkelijk/.

Has it been reported to the Dutch Personal Data Authority?

Yes, this has been a requirement since the introduction of the General Data Protection Regulation (GDPR). We reported this incident to the Dutch Personal Data Authority on 21 October.

I have some further questions.

If following this incident you still have some questions, please send them to the following email address: incident-response@owknotarissen.nl.

Our office can also be contacted by phone, but we ask you to contact us above all by email so that we can give you the best possible answer to your questions.