Current information about the data leaked (6 March 2023, 5:00 pm)

What personal information has been leaked?

The data is currently being analysed in order to determine which personal information has been stolen and published. Based on an initial review (6 March), the information published is from only a small number of users.

If your information has been published on the darknet, you will be personally notified. If you do not receive notification in the coming weeks, you can assume that you have not been impacted. We will also provide information here when the notification process is complete so that this is also clear to you.

Please note that at the moment we cannot provide individual answers to what is likely your most pressing question: Have I been impacted? The employees who are carrying out the analysis have also been instructed not to provide individual information. The detailed analysis of the data will take some time due to the number of files, but it will definitely be carried out as quickly as possible.

What other information has been leaked?

In addition to reviewing the published data for personal information, HAW Hamburg is also checking whether the data contains other sensitive information – e.g. from research projects, governance bodies or internal work units. Here, too, the relevant contact people at the university will be informed if the analysis provides information to this effect.

The university has already reviewed what security-relevant data may have been compromised through the cyber-attack. This took place in the direct aftermath of the attack.

How can I find out if my information has been published on the darknet?

If your information has been compromised as a result of the cyber-attack, you will be notified. If you do not receive notification in the coming weeks, you can assume that you have not been impacted.

At the current time, you can follow the advice of the Federal Office for Information Security and use the following Internet portals to enter your email address and check whether your personal login information has been published as part of known leaks:

- HPI Identity Leak Checker (German)
- haveibeenpwned.com (English)

If you receive a notification from one of these portals, this means that your email address has been published as part of one or more data leaks. This does not necessarily mean that the leak is linked to the incident at HAW Hamburg.

Where has the information been published?

The criminal group has published the information on the darknet. The darknet is a part of the Internet which cannot be found through the usual channels and is only accessible via specific browsers. Because darknet users are generally anonymous due to encryption mechanisms, the darknet is frequently used by criminals for communication or as a marketplace.

Can I look through the data published on the darknet myself to determine whether I've been impacted?

The files published on the darknet could contain hidden malware that may not be recognised by commonly used virus scanners. For this reason, IT security experts and the Federal Office for Information Security strongly recommend that you do not download, open or review the files.

Will my information be deleted from the darknet?

Criminal hacker groups generally operate anonymously on the darknet, and the servers are usually not located in Europe. It is therefore often not possible for law enforcement and regulatory authorities to delete the data or to deactivate the pages on the darknet where the information has been published.

What should I do now?

Please continue to follow the IT security guidelines provided on the university website following the cyber-attack. You should change your passwords as soon as possible, especially if you use the same password for several programmes or user accounts and have not yet changed it.

The criminals often use the data for fraudulent activities such as phishing mails or Internet purchases using false identities. We therefore ask you to be vigilant about suspicious emails and account activity in online shops.

We particularly ask that you do not open attachments or links in suspicious mails or answer such mails, especially those that indicate HAW Hamburg as the supposed sender and/or ask you to carry out unusual activities – e.g. transferring money to alternative accounts or changing your passwords.

If you are informed that your personal information has been leaked, please immediately take the steps recommended by the Federal Office for Information Security.

How can I protect myself in future?

Use only secure passwords and avoid using the same password for different programmes and user accounts. Two-step verification has been activated for MS Office 365 and other services. This provides additional protection and is also recommended for other sensitive applications – when the providers support it.

The Federal Office for Information Security has made the following recommendation for creating and using secure passwords.