Erpresser-E-Mails

Support

Bei Rückfragen oder Unsicherheiten im Zusammenhang mit Spam oder Phishing-E-Mails kontaktieren Sie bitte:

ZIM-Helpdesk

Tel.: +49 211 81-10111

E-Mail: helpdesk@hhu.de

Gebäude 25.41, Raum 00.53

Servicezeiten: Mo.-Fr. 8.30-18 Uhr

Melden von IT-Sicherheitsvorfällen

CERT (Computer Emergency Response Team)

E-Mail: cert@hhu.de

Weitere Sicherheitshinweise und Informationen

Sicherheitshinweise

Gefälschte Helpdesk-E-Mails

Spear-Phishing

CEO-Fraud-E-Mails

Melden von Spam- und Phishingmails

Blacklisting

Was sind Erpresser-E-Mails?

An HHU-Postfächer werden manchmal E-Mails verschickt, in denen der Absender behauptet, er hätte sich Zugang zum Endgerät des Empfängers verschafft und über die Webcam kompromittierende Aufnahmen angefertigt. Es wird mit der Veröffentlichung dieser Aufnahmen gedroht, sofern nicht ein bestimmter Geldbetrag, meist in Form von Bitcoin, gezahlt wird.

Was ist von diesen Erpresser-E-Mails zu halten?

Kurz gesagt: nichts.

Der Text der E-Mails an verschiedenste Empfänger ist immer derselbe und enthält keinerlei Informationen, wie sie ein Hacker bei einem tatsächlichen Zugriff auf ein Endgerät erlangt hätte.

Die Mails sind daher sichtlich darauf angelegt, eher unerfahrene Computernutzer:innen zu verunsichern und zur Zahlung eines Geldbetrags zu verleiten.

In keinem uns bislang bekannt gewordenen Fall konnte eine tatsächliche Kompromittierung eines Endgerätes nachgewiesen werden.

Wie sollte ich mich verhalten, wenn ich eine Erpresser-E-Mail erhalte?

Geraten Sie nicht in Panik! Überweisen Sie in solchen Fällen niemals Geld!

Sie können solche Mails bedenkenlos ignorieren und löschen bzw. in den "Spam"-Ordner Ihres Postfachs verschieben.

Im Zweifel kontaktieren Sie bitte den ZIM-Helpdesk oder das HHU-CERT (die Kontaktdaten finden Sie oben rechts auf dieser Seite).

Sollte sich ein Endgerät von Ihnen seltsam verhalten oder sollten Sie den Verdacht haben, dass Ihr Endgerät gehackt wurde, trennen Sie dieses vom Netz und führen Sie einen Virenscan durch. Ändern Sie die Zugangsdaten zu Ihren Accounts über einen anderen Rechner. Falls es sich um ein Dienstgerät handelt, informieren Sie bitte das HHU-CERT oder den Information Officer (IO) Ihrer Fakultät /Einrichtung, damit weitere Schritte abgestimmt werden können.

English version

What are blackmail emails?

Emails are sometimes sent to HHU mailboxes in which the sender claims to have gained access to the recipient's computer and made compromising recordings via the webcam. The sender threatens to publish these recordings unless a certain amount of money, usually in the form of Bitcoin, is paid.

What should I make of these blackmail emails?

In short: nothing.

The text of the emails sent to various recipients is always the same and does not contain any information that a hacker would have obtained by actually accessing a computer.

The emails are therefore clearly designed to unsettle inexperienced computer users and tempt them to pay a sum of money.

In none of the cases we have become aware of to date has it been possible to prove that a computer has actually been compromised.

What should I do if I receive a blackmail email?

Do not panic! Never transfer money in such cases!

You can safely ignore and delete such mails or move them to the "Spam" folder of your mailbox.

If in doubt, please contact the ZIM Helpdesk or the HHU-CERT (contact details can be found at the top right of this page).

If one of your end devices is behaving strangely or if you suspect that your end device has been hacked, disconnect it from the network and carry out a virus scan. Change the access data for your accounts via another computer. If it is a university owned computer, please inform the HHU-CERT or the Information Officer (IO) of your faculty/institution so that further steps can be coordinated.