CEO-Fraud-E-Mails

Inhalt / Content:

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

Was ist CEO-Fraud?

Im Gegensatz zu Phishing-Mails sind CEO-Fraud-Mails darauf ausgelegt, Geldbeträge zu erbeuten. Die Täter geben sich dafür als Vorgesetzte aus und bitten zielgerichtet Mitarbeiter:innen zunächst um Hilfe und dann in einem zweiten Schritt, über einen Link Geld für angebliche Gutscheine, Blumen oder andere Waren/Dienstleistungen vorzustrecken.

Wir verweisen hier auch auf die sehr gute Infoseite der Universität Münster zu diesem Thema: https://www.uni-muenster.de/IT-Sicherheit/news/deceptive-spam.html

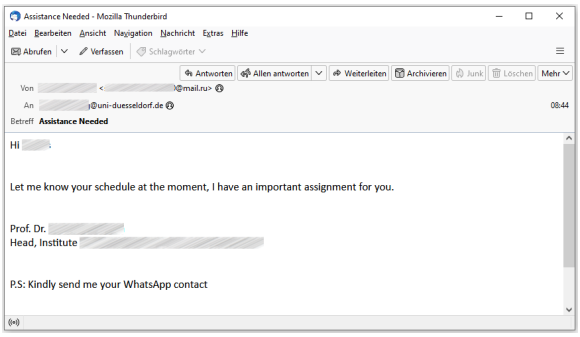
Melden von IT-Sicherheitsvorfällen

CERT (Computer Emergency Response Team)

E-Mail: cert@hhu.de

Woran erkenne ich CEO-Fraud-Mails?

- Hinter dem Namen des Absenders steht eine abweichende E-Mail-Adresse, meist von Gmail oder Mail.ru. Wenn Ihr E-Mail-Programm nur den Absendernamen, nicht aber die Adresse anzeigt, klicken Sie den Absendernamen an bzw. gehen Sie mit dem Mauszeiger darauf, dann wird die Adresse angezeigt.
- Die E-Mails sind meist auf Englisch verfasst, selbst dann, wenn die Bürokommunikation sonst nie in einer Fremdsprache erfolgt.
- Wenn Sie auf die E-Mail antworten, werden Sie in einer zweiten Mail aufgefordert, über einen Link Geld für angebliche Gutscheine oder andere Waren/Dienstleistungen zu überweisen.



Beispiel für eine CEO-Fraud-Mail.

Weitere Sicherheitshinweise und Informationen

Sicherheitshinweise

Gefälschte Helpdesk-E-Mails

Spear-Phishing

Melden von Spam- und Phishingmails

Blacklisting

Was tun, wenn ich eine CEO-Fraud-Mail erhalte?

Bitte beantworten Sie die Mail nicht und löschen Sie diese bzw. (wenn Sie ein Roundcube-Postfach haben) verschieben Sie die Nachrichten in den "Spam"-Ordner Ihres Online-Postfachs - auf diesem Weg helfen Sie, den Spamfilter zu trainieren. Nutzer:innen von Exchange können solche Mails an spamreport@hhu.de melden.

Fragen Sie bei ungewöhnlichen E-Mails Ihre/Ihren Vorgesetzte/n, ob die Mail tatsächlich von ihr/ihm stammt.

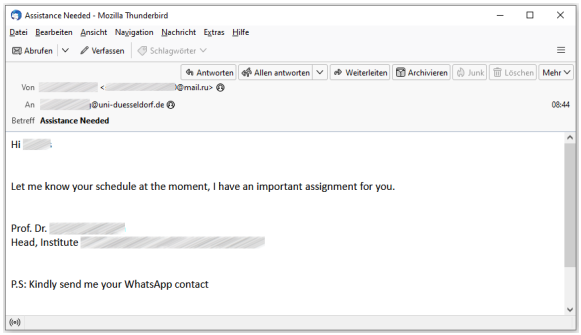
English version

What is CEO-Fraud?

In contrast to phishing e-mails, CEO fraud e-mails are designed to obtain sums of money. The perpetrators pose as supervisors and ask targeted employees for help and then, in a second step, to advance money via a link for alleged vouchers, flowers or other goods/services.

How can I recognise CEO fraud emails?

- Behind the sender's name is a different e-mail address, usually from Gmail or Mail.ru. If your e-mail programme only displays the sender's name but not the address, click on the sender's name or move the mouse pointer over it and the address will be displayed.
- Emails are mostly written in English, even when office communication is otherwise never in a foreign language.
- If you reply to the email, a second email will ask you to transfer money via a link for alleged vouchers or other goods/services.



Example of a CEO fraud mail.

What should I do if I receive a CEO Fraud email?

Please do not reply to the mail and delete it or (if you have a Roundcube mail box) move the messages to the "Spam" folder of your online mailbox - this way you help to train the spam filter. Exchange user can report such mails to spamreport@hhu.de.

In case of unusual e-mails, ask your supervisor if the e-mail really comes from him/her.