Spam und Phishing im Namen von TU E-Mail-Adressen

05.01.2025 07:57:54

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	14:22:58 - 12.10.2017

Schlüsselwörter

Spam Phishing E-Mail gefälscht

Symptom (öffentlich)

Es werden im Namen von TU-Mitgliedern gefälschte E-Mails (insbesondere Spam und Phishing) verschickt.

Beispiel: Von: mustermann.max@institut.tu-darmstadt.de [mailto:spammer@fremdeurl.com])

Problem (öffentlich)

Leider kann das HRZ hier derzeit nichts tun. Es ist vergleichbar dem Absender auf einem Brief, hier kann jeder einfach einen Namen aufschreiben und behauptet damit, dass diese Person der Absender sei.

Lösung (öffentlich)

Das Verfahren wird bei Phishing sehr intensiv angewendet um an Whitelist-Mechanismen vorbei an die Empfänger zu kommen. Bitte behandeln sie solche Nachrichten mit Vorsicht und wenn eine Nachricht unerwartet ist, dann öffnen sie keine Anhänge und fragen sie vorher nach. Im Zweifelsfall löschen Sie die Nachricht.

Für die Praxis ein paar hilfreiche Tipps im Umgang mit gefälschten E-Mails:

- Den Adressaten kritisch betrachten. Stimmt z.B. der Anzeigename mit der E-Mail-Adresse überein? Beispiel: Von: mustermann.max@institut.tu-darmstadt.de [mailto:spammer@fremdeurl.com]
- Keine seltsamen Links öffnen. Immer genau schauen, wo der Link wirklich hinführt.
- Keine unbekannten Anhänge öffnen (vor allem keine ausführbaren Dateien z.b. exe, und keine Makros aktivieren)

Weitere Informationen und Hinweise haben wir für Sie auf der Homepage: [1]https://www.hrz.tu-darmstadt.de/phishing

[1] https://www.hrz.tu-darmstadt.de/phishing