Vorsicht!

Geschätzte Mitarbeitende

Derzeit erreicht Nutzern eine neue Welle von Betrugsmails. Diese zielen darauf ab, persönliche Daten wie Login zu erhalten oder über einen Link respektive Anhang Ihren Computer zu infizieren.

Um die Nachrichten so vertrauenswürdig wie möglich aussehen zu lassen, verwenden die Kriminellen zudem echte Daten der Empfänger, beispielsweise Namen, Adresse sowie Inhalt vom Mail.

Fake-Mails erkennen:

- Falsche Absenderadresse: Deshalb nach Tippfehlern beim Absender suchen.
- Zum Beispiel: "jasimn.hot@schulthess.ch" statt "jasmin.hot@schulthess.ch".
- Im Zweifelsfall den Mauszeiger auf die Absenderleiste führen, so lässt sich mithilfe des sogenannten "mouseover" die hinterlegte Absenderadresse anzeigen.
- Den Inhalt der Mail ebenfalls genau anschauen, bei Verdacht die IT informieren.
- Es ist darauf zu achten, dass nur vertrauenswürdige E-Mail-Attachments geöffnet werden (in letzter Konsequenz sogar nach telefonischer Absprache mit dem Absender).
- Unbekannte Links nicht anklicken

Kontaktieren Sie bei einem Verdacht oder im Zweifelsfall umgehend die IT.

Besten Dank für Eure aktive Mithilfe!

Eure IT Abteilung

29.08.2019