TECHNISCHE UNIVERSITÄT DARMSTADT

Betrügerische Nachrichten

Wie Sie Phishing-Nachrichten und andere betrügerische Nachrichten erkennen

IT-Sicherhe!t

Informationssicherheit | TU Darmstadt

HRZ Hochschulrechenzentrum

SECUSO SECURITY · USABILITY · SOCIETY

KASTEL

Allgemeine Informationen

Kriminelle nutzen verschiedene Strategien, um Ihnen zu schaden. Beliebte Angriffsstrategien sind

- die Verbreitung von Schadsoftware, um z. B. Zugriff auf Ihre Geräte zu erlangen oder
- das Täuschen der Endanwender, um an sensible Informationen zu gelangen (z. B. an Zugangsdaten).

Eine weit verbreitete Angriffsmethode ist es, betrügerische Nachrichten zu verschicken, die Ihnen einen legitimen Grund für die Nachricht an Sie vorgaukeln. Solche Nachrichten können Sie über unterschiedliche Kanäle empfangen, z. B. als Telefonanruf, E-Mail, SMS, Nachricht über Messenger bzw. soziale Netzwerke.

Die Inhalte dieser Nachrichten können auf unterschiedliche Art und Weise gefährlich sein:

Sensible Daten: Nachrichten fordern Sie auf, sensible Daten wie Zugangsdaten oder schützenswerte Dokumente zu schicken.

Überweisungen/Anrufe: Nachrichten fordern Sie auf, Überweisungen oder Anrufe, z. B. an Kooperationspartner, vermeintliche Freunde oder Geschäfttftspartner, zu tätigen. So erhalten die Kriminellen eine direkte Überweisung von Ihnen oder der Betrag wird über die Telefonrechnung abgebucht.

Links: Nachrichten können einen oder mehrere gefährliche Links enthalten (diese Form betrügerischer Nachrichten wird auch als Phishing-Nachricht bezeichnet). Ziel des Betrugs ist es, dass Sie auf einen der Links klicken. Diese Links leiten Sie z. B. zu einer echt aussehenden, aber betrügerischen Webseite (auch als Phishing-Seite bezeichnet), bei der Sie sich einloggen sollen. Alternativ werden Sie zu einer Webseite weitergeleitet, die Ihnen auf Ihrem Gerät Schadsoftware installiert.

Anhänge: Nachrichten enthalten eine oder mehrere gefährliche Dateien (wie z. B. einen Anhang in einer E-Mail). Ziel der Betrüger ist es, dass Sie den Anhang öffnen. Durch das Öffnen bzw. Ausführen der Datei wird auf Ihrem Gerät Schadsoftware installiert.

Werbung: Nachrichten enthalten Werbung oder sonstige wertlose Inhalte (diese Nachrichten werden häufig als Spam bezeichnet). Ziel des Angriffs ist es, dass Sie etwas kaufen. Der primäre Schaden ist in der Realität jedoch die verlorene Arbeitszeit, weil Sie die Nachricht kurz ansehen, bewerten und dann löschen.

Gemeinsam gegen betrügerische Nachrichten

Das Hochschulzentrum (HRZ) der TU Darmstadt setzt technische Maßnahmen ein, um betrügerische Nachrichten, die in das TUDa-Netz gelangen, automatisiert zu erkennen. Diese werden Ihnen erst gar nicht zugestellt oder landen direkt im Spam-Ordner. Leider ist es mit den existierenden Maßnahmen nicht möglich, alle betrügerischen Nachrichten zu entdecken. Da die Angriffsmethoden immer besser werden, sind viele betrügerische Nachrichten immer schwerer zu entdecken. Außerdem hätten zu strikte Regeln die Konsequenz, dass auch Nachrichten nicht zugestellt werden, die gar nicht betrügerisch sind, aber zufällig ähnliche Eigenschaften wie betrügerische Nachrichten aufzeigen.

Daher ist es wichtig, dass Sie Ihre E-Mails sorgfältig prüfen und bei der Entdeckung betrügerischer E-Mails mithelfen.

Ihre Mitarbeit ist ein wichtiger Bestandteil, um die IT-Sicherheit an der TU Darmstadt sicherzustellen.

In diesem Faltblatt finden Sie sowohl allgemeine Informationen über betrügerische Nachrichten, als auch sieben Regeln, wie Sie solche Nachrichten erkennen.

Das IT-Sicherheitsteam hilft – Melden Sie sich!

Im Alltag liegt Ihr Fokus nicht immer auf der Prüfung von Nachrichten. Wenn Sie daher doch einmal auf eine betrügerische Nachricht hereinfallen und es anschließend merken, kontaktieren Sie umgehend das IT-Sicherheitsteam der TU Darmstadt (siehe Kontakt auf der Rückseite des Flyers). Melden Sie sich auch, wenn Sie unsicher sind. Das IT-Sicherheitsteam wird Ihnen helfen. Mit dem (schnellen) Reagieren auf betrügerische Nachrichten tragen Sie dazu bei, das Ausmaß des Schadens für Sie und andere an der TU Darmstadt so gering wie möglich zu halten.

Wenn Sie zukünftig eine betrügerische Nachricht klar als solche erkennen, dann löschen Sie diese Nachricht unmittelbar. Wenn Sie eine Nachricht erhalten, bei der Sie sich unsicher sind, ob diese eine betrügerische ist, dann schicken Sie diese Nachricht mit der Bitte um Unterstützung an phishing@tu-darmstadt.de.

Kontakt

Stabsstelle IT-Sicherheit an der TU Darmstadt
https://www.tu-darmstadt.de/it-sicherheit/

Zentraler IT-Sicherheitsbeauftragter der TU Darmstadt

Dr.-Ing. Johannes Braun
itsb@tu-darmstadt.de
+49 6151 16-71151

Computer Emergency Response Team (TUDa-CERT)

Jochen Becker
cert@tu-darmstadt.de
+49 6151 16-71021

Meldung von verdächtigen E-Mails / Phishing E-Mails

phishing@tu-darmstadt.de

Meldung von IT-Sicherheitsvorfällen

security@hrz.tu-darmstadt.de

Im IT-Sicherheitsnotfall

+49 6151 27777

Urheber: Karlsruher Institut für Technologie (KIT), Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), Forschungsgruppe Security o Usability o Society (SECUSO). https://secuso.aifb.kit.edu/

Der Inhalt des Faltblatts basiert auf Erkenntnissen aus dem Projekt „KMU AWARE – Awareness im Mittelstand“, welches die Forschungsgruppe SECUSO an der TU Darmstadt durch-geführt hat und welches im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie bis zum 31.03.2018 gefördert wurde. Die Finanzierung des Faltblatts erfolgt im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts KASTEL.

Folgende Regeln helfen Ihnen, betrügerische Nachrichten zu erkennen

1. Regel: Prüfen Sie Absender und Inhalt jeder Nachricht auf Plausibilität!

- Passt der Absender nicht zur Nachricht?
  - ✓ Der Absender info@**secuso.org** ist bei einer SECUSO E-Mail plausibel.
  - ✗ Der Absender info@**sye.jp** ist bei einer SECUSO E-Mail nicht plausibel.
- Werden sensible Daten abgefragt?
- Werden Sie aufgefordert, Geld zu überweisen oder jemanden anzurufen, wobei in der Nachricht die dafür nötigen Informationen angegeben sind?
- Haben Sie dort kein Nutzerkonto?
- Erhalten Sie die Nachricht unerwartet?
- Ist die Anrede falsch oder passt diese nicht zum Absender?
- Im Fall von E-Mails: Ist die E-Mail von der entsprechenden Person nicht digital signiert?

Je mehr Fragen Sie mit „ja" beantworten können, desto wahrscheinlicher ist es, dass es sich um eine betrügerische Nachricht handelt. Besondere Vorsicht ist bei den sensiblen Daten inkl. Passwörtern geboten. Stellen der TU Darmstadt, bspw. das HRZ oder der IT-Sicherheitsbeauftragte, würden Sie nicht auffordern, ihnen Ihr Passwort zu senden.

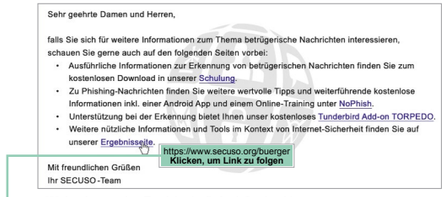
Übrigens: Die meisten der obigen Fragen können Sie auch auf den Telefon-, Fax- bzw. Briefpost-Kontext anwenden.

2. Regel: Machen Sie sich damit vertraut, wo Sie die tatsächliche Webadresse hinter einem Link finden!

Bevor Sie voreilig auf einen Link klicken, untersuchen Sie diesen. Ein Link kann meist daran erkannt werden, dass der Text blau und unterstrichen ist. Jedoch können Links auch in Form von Buttons oder Bildern in Nachrichten integriert sein.

Zunächst sollten Sie herausfinden, welche Webadresse (auch URL genannt) tatsächlich hinter dem Link steckt. Diese Information ist je nach Gerät, Software und Dienst (z. B. Amazon, Dropbox, WhatsApp, Facebook, Xing) an unterschiedlichen Stellen zu finden. Sie sollten sich also vor der Nutzung eines Geräts, einer Software bzw. eines Dienstes damit vertraut machen, wo die tatsächliche Webadresse eines Links zu finden ist.

Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren, ohne ihn anzuklicken. Der Link erscheint entweder in der Statusleiste oder in einem Infofeld (auch Tooltip genannt).



Webadresse im Tooltip (z. B. bei Outlook)

Webadresse in der Statusleiste (z. B. bei Thunderbird oder Webbrowsern wie Firefox, Internet Explorer und Chrome)

Bei mobilen Geräten (Smartphones und Tablets) hängt das Vorgehen zum Identifizieren der Webadresse eines Links stark vom Gerät und von der jeweiligen App ab. Meist ist es so: Wenn Sie Ihren Finger für mindestens 2 Sekunden auf dem Link halten, dann wird die Webadresse im Dialogfenster angezeigt. Achten Sie darauf, dass Sie den Link dabei nicht versehentlich anklicken. Wenn Sie unsicher sind, warten Sie, bis Sie wieder an Ihrem PC oder Laptop sind.

Webadresse im Dialogfenster (Betriebssystem iOS)

Webadresse im Dialogfenster (Betriebssystem Android)

3. Regel: Identifizieren Sie den sogenannten Wer-Bereich in der Webadresse!

https://nophish.**secuso.org**/login

Wer-Bereich

Der Wer-Bereich einer Webadresse besteht aus den zwei durch einen Punkt getrennten Begriffen, die entweder direkt vor dem ersten alleinstehenden Schrägstrich „/" stehen, falls ein solcher vorhanden ist, andernfalls ganz am Ende der Webadresse. Der Wer-Bereich ist der wichtigste Indikator für die Erkennung gefährlicher Webadressen und damit von Nachrichten mit gefährlichen Links. In der Fachsprache wird er „Domain" genannt. Falls hier Zahlen stehen, handelt es sich um eine sogenannte IP-Adresse und es ist höchstwahrscheinlich eine gefährliche Webadresse.

✗ https://**129.13.152.9**/secuso.org.secure-login.de/

Übrigens: Auch Kriminelle nutzen inzwischen https.

4. Regel: Prüfen Sie, ob der Wer-Bereich zur (vermeintlich) legitimen Nachricht passt!

Wenn der Wer-Bereich nicht zum Absender, Betreff oder Inhalt passt oder nicht korrekt geschrieben ist, klicken Sie nicht auf den Link. Es handelt sich sehr wahrscheinlich um eine betrügerische Nachricht.

Im Fall, dass Sie z.B. erwarten, dass der Link Sie zu Seiten der TU Darmstadt führt:

✓ https://www.**tu-darmstadt.de**/it-sicherheit

✗ https://www.**t-u-d.de**/it-sicherheit

Übrigens: Kriminelle schreiben den zu erwartenden Wer-Bereich an eine andere Stelle in die Webadresse, um Sie zu täuschen:

✓ https://www.**mein-paketservice.de**/

✗ https://mein-paketservice.de.**shoppen-im-web.de**/

✗ https://**shoppen-im-web.de**/mein-paketservice.de/

✗ https://mein-paketservice.de.**s-o-k.de**/login

Übrigens: Kriminelle registrieren Wer-Bereiche, die mit dem eigentlichen Wer-Bereich bis auf wenige Zeichen übereinstimmen.

✓ https://www.**bauernmarkt-total.de**

✗ https://www.**baurenmarkt-total.de**

✗ https://www.**bauermarkt-total.de**

✗ https://www.**bauernrnarkt-total.de**

5. Regel: Wenn Sie den Wer-Bereich nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suchmaschine!

✓ https://www.**secuso.org**/

✗ https://www.**secuso-research.de**/

6. Regel: Prüfen Sie das Dateiformat des Anhangs!

Anhänge könnten potenziell (sehr) gefährliche Dateiformate haben, solche sind:

- Direkt ausführbare Dateiformate (sehr gefährlich): z. B. .exe, .bat, .com, .cmd, .scr, .pif
- Dateiformate, die Makros enthalten können: z. B. Microsoft Office Dateien wie .doc, .docx, .docm, .ppt, .pptx, .xls, .xlsx
- Dateiformate, die Sie nicht kennen

7. Regel: Wenn das Dateiformat potenziell (sehr) gefährlich ist, dann öffnen Sie den Anhang nur, wenn Sie diesen genauso von dem Absender erwarten!

Falls Sie unsicher sind, ob Sie die Nachricht einfach löschen können, holen Sie weitere Informationen ein. Dabei verwenden Sie auf keinen Fall die Kontaktmöglichkeiten aus der Nachricht. Rufen Sie z. B. den Absender an.

Wenn Sie bei Office-Programmen nach dem Öffnen gefragt werden, ob Makros ausgeführt werden sollen, ist dies ein guter Zeitpunkt, erneut zu überlegen, ob die Nachricht, aus der die Datei stammt, nicht doch eine betrügerische Nachricht ist. Brechen Sie den Vorgang erst einmal ab.

Weitere Informationen

Auf unserer Webseite erhalten Sie weitere Informationen und Details wie Sie betrügerische Nachrichten erkennen, inkl. Erklärvideos, Online-Quiz und Security-Game zum spielerischen Selbsttest.

www.tu-darmstadt.de/it-sicherheit/phishing

Übrigens: Wenn Sie Rückmeldungen erhalten, dass jemand eine E-Mail von Ihnen erhalten hat, die Sie gar nicht verschickt haben, informieren Sie ebenfalls das IT-Sicherheitsteam der TU Darmstadt. Dann werden wir gemeinsam das Problem beheben.