Allgemeine Informationen zu betrügerischen Nachrichten

Internetbetrüger nutzen verschiedene Strategien, um Ihnen und/oder Ihrem Unternehmen zu schaden. Hierunter fallen beispielsweise die Verbreitung von Schadsoftware oder das Täuschen, um an sensible Informationen zu gelangen (z. B. Zugangsdaten). Eine beliebte und weit verbreitete Methode ist es, Ihnen betrügerische Nachrichten mit gefährlichen Inhalten zu schicken. Dabei kann es sich um folgende Inhalte handeln:

1.) Die Nachrichten fordern Sie auf mit verschiedenen sensiblen Daten wie Zugangsdaten oder Kreditkartendaten zu antworten. Ziel der Betrüger ist es hierbei, an die geforderten Informationen zu gelangen und diese womöglich zu missbrauchen.

2.) Die Nachrichten fordern Sie auf Überweisungen oder Anrufe, z. B. an vermeintliche Geschäftspartner, zu tätigen.

3.) Vorsicht: Die Angabe einer Webadresse als Link in der Nachricht kann manipuliert sein. Daher ist es wichtig, die tatsächliche Webadresse auch hinter diesem Link zu prüfen. Die Nachrichten enthalten einen oder mehrere gefährliche Links. Ziel der Betrüger ist es hierbei, dass Sie auf einen der Links klicken. Diese Links leiten Sie dann z. B. zu einer betrügerischen aber authentisch aussehenden Webseite, bei der Sie sich einloggen sollen, oder zu einer Webseite, die Ihnen auf Ihrem Gerät Schadsoftware installiert. Solche Links müssen Sie nicht einmal zur direkten Eingabe von Daten auffordern. Bereits Nachrichten, die Sie lediglich auf Informationen hinweisen, können gefährliche Links enthalten.

4.) Die Nachrichten enthalten eine gefährliche Datei (z. B. einen Anhang in einer E-Mail). Ziel der Betrüger ist es hierbei, dass Sie den Anhang öffnen bzw ausführen. Durch das Öffnen bzw. Ausführen wird auf Ihrem Gerät bereits Schadsoftware installiert.

Kontakt

Karlsruhe Institut für Technologie (KIT)

Institut für Angewandte Informatik und
Formale Beschreibungsverfahren (AIFB)

Forschungsgruppe Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gbd. 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-mail: kontakt@secuso.org

www.aifb.kit.edu/web/SECUSO
www.facebook.com/secuso
twitter.com/secusotu

Herausgeber

Karlsruher Institut für Technologie (KIT)

President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

© SECUSO 12/02/2018
Die Unterlagen sind urheberrechtlich geschützt.

Der Inhalt des Flyers basiert auf Erkenntnissen aus dem Projekt „KMU AWARE – Awareness im Mittelstand“, welches die Forschungsgruppe SECUSO an der TU Darmstadt durchführt und welches im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie noch bis zum 31.03.2018 gefördert wird.

Karlsruhe Institute of Technology

aifb

Online-Betrug

Wie Sie betrügerische Nachrichten im Internet erkennen können

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

Folgende Regeln helfen Ihnen betrügerische Nachrichten zu erkennen

1. Regel: Prüfen Sie Absender und Inhalt jeder empfangenen Nachricht auf Plausibilität (z. B. passt der Absender zur Nachricht, werden sensible Daten abgefragt oder haben Sie dort überhaupt ein Nutzerkonto). Falls die Nachricht unplausibel ist, löschen Sie diese!

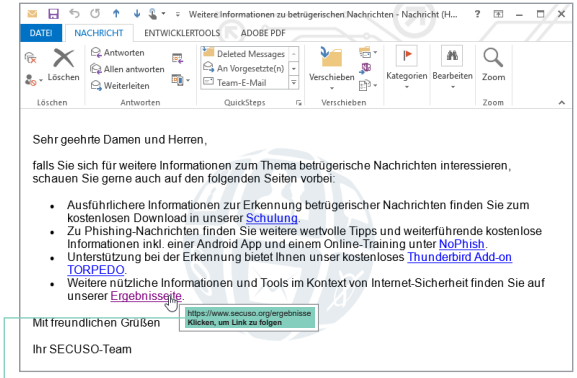
✗ Der Absender shop@sye.jp ist bei einer Amazon E-Mail nicht plausibel.

✓ Der Absender rechnung@amazon.de ist bei einer Amazon E-Mail plausibel.

2. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Link enthält, prüfen Sie, ob es sich um eine gut gemachte betrügerische Nachricht handelt und die Nachricht z. B. gar nicht vor dem (vermeintlichen) Absender stammt. Dazu müssen Sie zunächst heraus finden, welche Webadresse tatsächlich hinter dem Link steckt, bevor Sie darauf klicken.

Die Information, welche Webadresse tatsächlich hinter einem Link steckt, ist je nach Gerät, Software und Dienst (z. B. Amazon, Dropbox, Skype, WhatsApp, Facebook, Google+, Xing, LinkedIn) 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. Ein Link kann meist daran erkannt werden, dass der Text blau hinterlegt und unterstrichen ist.

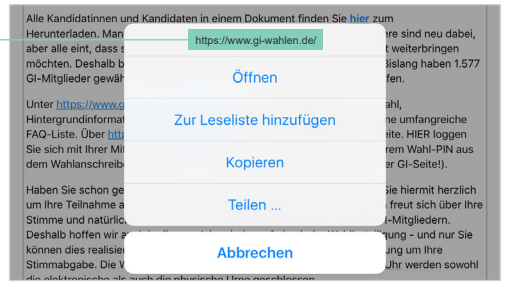
Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren, ohne ihn aber zu klicken. Der Link wird entweder in der Statusleiste am Fuß des Fensters, oder in dem Infofeld, welches auch Tooltip genannt wird, erscheinen. Beispiele dazu finden Sie in folgenden Abbildungen:



Webadresse im Infofeld (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, dass Sie für mindestens 2 Sekunden mit dem Finger auf dem Link verweilen oder diesen für mindestens 2 Sekunden drücken. Achten Sie darauf, dass Sie den Link dabei nicht versehentlich klicken, d. h. kurz antippen. Dadurch wird die Webadresse oben in einem Dialogfenster angezeigt:



Webadresse im Dialogfenster (Betriebsystem iOS)

3. Regel: Wenn Sie die Webadresse hinter dem Link gefunden haben, identifizieren Sie als nächstes den sogenannten Wer-Bereich in der Webadresse.

https://nophish.secuso.org/login

Wer-Bereich

Der Wer-Bereich besteht immer aus den letzten beiden Begriffen vor dem ersten alleinstehenden „/" (in diesem Fall secuso.org) einer Webadresse. Der Wer-Bereich ist der wichtigste Bereich 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 daher wahrscheinlich um eine gefährliche Webadresse.

4. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, prüfen Sie, ob der Wer-Bereich einen Bezug zu dem (vermeintlichen) Absender und dem Inhalt der Nachricht hat und ob er korrekt geschrieben ist. Wenn nur eines davon zutrifft, dann folgen Sie diesem Link nicht!

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

✗ http://shoppen-im-web.de/mein-paketservice.de/

✓ https://www.mein-paketservice.de/

✗ https://www.130.83.167.22/secuso.org.secure-login.de/

✗ https://www.mein-paketsrevice.de/

✓ https://www.mein-paketservice.de/

✗ https://www.secureqay24.de/

✓ https://www.securepay24.de/

5. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, Sie den Wer-Bereich aber nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suchmaschine. Wenn Sie den Wer-Bereich nicht als vertrauenswürdig einstufen, löschen Sie die Nachricht!

✗ https://www.secuso-research.org/

✓ https://www.secuso.org/

6. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Anhang enthält, dann prüfen Sie, ob dieser Anhang ein potentiell (sehr) gefährliches Dateiformat hat. Potentiell gefährliche Dateiformate 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, .ppt, .pptx, .xls, .xlsx.
- Dateiformate, die Sie nicht kennen.

7. Regel: Wenn das Dateiformat potentiell (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, sollten Sie weitere Informationen einholen, dabei aber nicht die Kontaktmöglichkeiten aus der Nachricht verwenden. Rufen Sie z. B. den Absender an.