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 der Endanwender, um an sensible Informationen zu gelangen (z. B. an Zugangsdaten). Eine beliebte und weit verbreitete Methode ist es, Ihnen betrügerische Nachrichten zu schicken, die Ihnen einen legitimen Grund für die Nachricht an Sie vorgaukeln. Wenn betrügerische Nachrichten es zum Ziel haben, sensible Informationen abzugreifen, dann nennt man diese Nachrichten Phishing-Nachrichten. Betrügerische Nachrichten können Sie über unterschiedliche Kanäle empfangen, z. B. als E-Mail, SMS, Nachricht über Messanger 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, schützenswerte Dokumente oder Kreditkartendaten, zurück zu schicken. Diese Nachrichten beinhalten oft eine Drohung oder eine Versprechung, um Sie zu überzeugen, schnell und damit unüberlegt sensible Daten zu verschicken.

Überweisungen/Anrufe: Nachrichten fordern Sie auf, Überweisungen oder Anrufe, z. B. an vermeintliche Freunde oder Geschäftspartner, zu tätigen. Hierbei ist es das Ziel der Betrüger, von Ihnen einen bestimmten Geldbetrag zu ergaunern. So erhalten die Betrüger eine direkte Überweisung von Ihnen oder der Betrag wird über Ihre Telefongesellschaft mit der nächsten Abrechnung abgebucht.

Links: Nachrichten können einen oder mehrere gefährliche Links enthalten. Ziel des Betrugs ist es, dass Sie auf einen der Links klicken. Diese Links leiten Sie dann 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, dass Sie den Anhang öffnen. Durch das Öffnen bzw. Ausführen der Datei wird auf Ihrem Gerät 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.secuso.aifb.kit.edu
facebook.com/secuso
twitter.com/secusoresearch

Herausgeber

Karlsruher Institut für Technologie (KIT)

Präsident Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.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 durchgeführt 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.

Karlsruher Institut für Technologie

aifb

Betrügerische Nachrichten

Wie Sie betrügerische Nachrichten und insbesondere Phishing-Nachrichten 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: Passt der Absender zur Nachricht? Werden sensible Daten abgefragt? Oder haben Sie dort überhaupt ein Nutzerkonto? Falls die Nachricht unplausibel ist, handelt es sich höchstwahrscheinlich um eine betrügerische Nachricht: löschen Sie diese Nachricht!

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

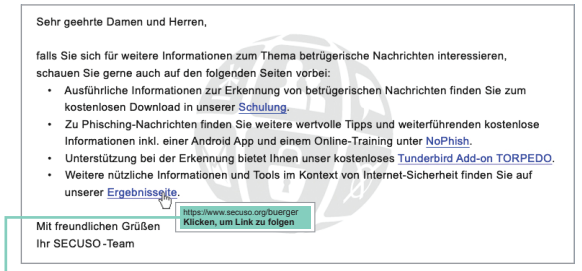
✓ Der Absender rechnung@amazon.com ist bei einer Amazon E-Mail plausibel.

2. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen oder mehrere Links enthält, prüfen Sie, ob es sich um eine gut gemachte betrügerische Nachricht handelt, bei der jemand vorgibt, der (vermeintliche) Absender zu sein, bevor Sie voreilig auf einen der Links klicken.

Ein Link kann meist daran erkannt werden, dass der Text blau und unterstrichen ist. Jedoch können Links die verschiedensten Erscheinungsformen haben. So können Sie z. B. in Form von Buttons, Wörtern in den unterschiedlichsten Farben oder einem Bild hinterlegt sein.

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.

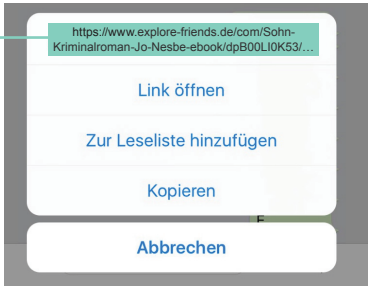
Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren, ohne ihn anzuklicken. Der Link wird entweder in der Statusleiste am Fuß des Fensters oder in dem Infofeld, welches auch Tooltip genannt wird, erscheinen.



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 klicken.



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.

http://nophish.secuso.org/login

Wer-Bereich

Der Wer-Bereich besteht immer aus den letzten beiden durch die Punkte getrennten Begriffe 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 es ist höchstwahrscheinlich 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 Absender oder Betreff nicht zum Inhalt passen, dann klicken Sie nicht auf den Link.

✓ https://www.mein-paketservice.de/

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

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

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

✓ https://www.bauernmarkt-total.de/

✗ https://www.baurenmarkt-total.de/

✗ https://www.bauemmarkt-total.de/

✗ https://www.bauerrnmarkt-total.de/

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

✓ https://www.secuso.org/

✗ https://www.secuso-research.org/

6. Regel: Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Anhang enthält, dann prüfen Sie, ob dieser Anhang ein potenziell (sehr) gefährliches Dateiformat hat. Potenziell 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 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, sollten Sie weitere Informationen einholen. Dabei verwenden Sie auf keinen Fall die Kontaktmöglichkeiten aus der Nachricht. Rufen Sie z. B. den Absender an.