Allgemeine Informationen

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

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

Eine weit verbreitete Angriffsmethode ist es, Ihnen betrügerische Nachrichten zu schicken, die Ihnen einen legitimen Grund für die Nachricht an Sie vorgaukeln. Betrügerische Nachrichten können Sie über unterschiedliche Kanäle empfangen, z. B. als 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 zurückzuschicken.

Überweisungen/Anrufe: Nachrichten fordern Sie auf, Überweisungen oder Anrufe, z. B. an Kooperationspartner, vermeintliche Freunde oder Geschäftspartner, 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. Ziel des Betrugs ist es, dass Sie auf einen der Links klicken. Diese Links leiten Sie dann z. B. zu einer echt ausse-henden, 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.

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.

Kontakt

Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)
Institut für Angewandte Informatik
und Formale Beschreibungsverfahren (AIFB)

Forschungsgruppe Security • Usability • Society (SECUSO)

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

Telefon: +49 721 608 450 45
E-Mail: secuso@aifb.kit.edu

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
https://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 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.

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 Nachricht auf Plausibilität: 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? Ist die E-Mail von der entsprechenden Person nicht digital signiert? Passt der Absender nicht zur Nachricht?

✗ Absender shop@sye.jp bei einer Amazon E-Mail

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

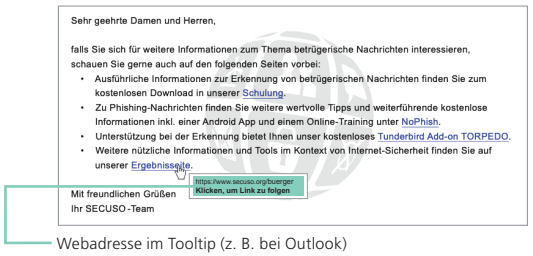
Je mehr Fragen Sie mit ja beantworten können, desto wahrscheinlicher ist eine betrügerische Nachricht. Besondere Vorsicht ist bei den sensiblen Daten inkl. Passwörtern gefragt.

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, d. h. bei der jemand vorgibt, der (vermeintliche) Absender zu sein, bevor Sie voreilig auf einen der Links klicken. Dazu untersuchen Sie den Link.

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.

Um den Link zu untersuchen, müssen Sie zunächst herausfinden, welche Webadresse (auch URL genannt) tatsächlich hinter dem Link steckt. Diese Information ist je nach Gerät, Software und Dienst (z. B. Amazon, Dropbox, Skype, 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.

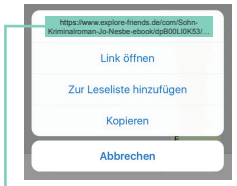
Bei PCs und Laptops erscheinen die Webadressen in der Regel, wenn Sie mit der Maus den Link berühren, ohne ihn anzuklicken. Der Link wird entweder in der Statusleiste oder in einem Infofeld (auch Tooltip genannt) erscheinen.



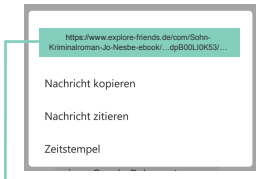
Webadresse im Tooltip (z. B. bei Outlook)

Webadresse in der Statusleiste (z. B. Thunderbird oder Webbrowsern)

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.



Webadresse im Dialogfenster (iOS)



Webadresse im Dialogfenster (Android)

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 durch die Punkte getrennten 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 es ist höchstwahrscheinlich eine gefährliche Webadresse.

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

4. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, prüfen Sie, ob der Wer-Bereich einen Bezug zu dem (vermeintlichen) Absender hat.

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

✓ https://www.mein-paketservice.de/

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

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

5. Regel: Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, prüfen Sie, ob der Wer-Bereich korrekt geschrieben ist.

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.bauemmarkt-total.de/

✗ https://www.bauerrnmarkt-total.de/

6. 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.

✓ https://www.secuso.org/

✗ https://www.secuso-research.org/

7. 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, .docm, .ppt, .pptx, .xls, .xlsx
- Dateiformate, die Sie nicht kennen

8. 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.

Wenn Sie bei Office-Programmen nach dem Öffnen gefragt werden, ob sogenannte 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.