Deutsche Bank

Private Guide #4 / Oktober 2020

So schützen Sie sich vor Phishing

Smarte Tipps gegen Cyber-Betrug

#PositiverBeitrag

Deutsche Bank

Lassen Sie sich nicht täuschen!

Mit ständig neuen Methoden versuchen Cyber-Kriminelle, Ihnen Passwörter zu entlocken oder Sie zu Handlungen zu verleiten, bei denen Ihre Geräte mit Schadprogrammen infiziert werden. „Phishing“ wird diese Masche genannt – eine Kombination aus den englischen Wörtern „password“ und „fishing“. Die Tipps dieses smarten Ratgebers helfen, solche Angriffe zu erkennen und Ihre Daten vor Missbrauch zu schützen.

Angriffe über alle Kanäle

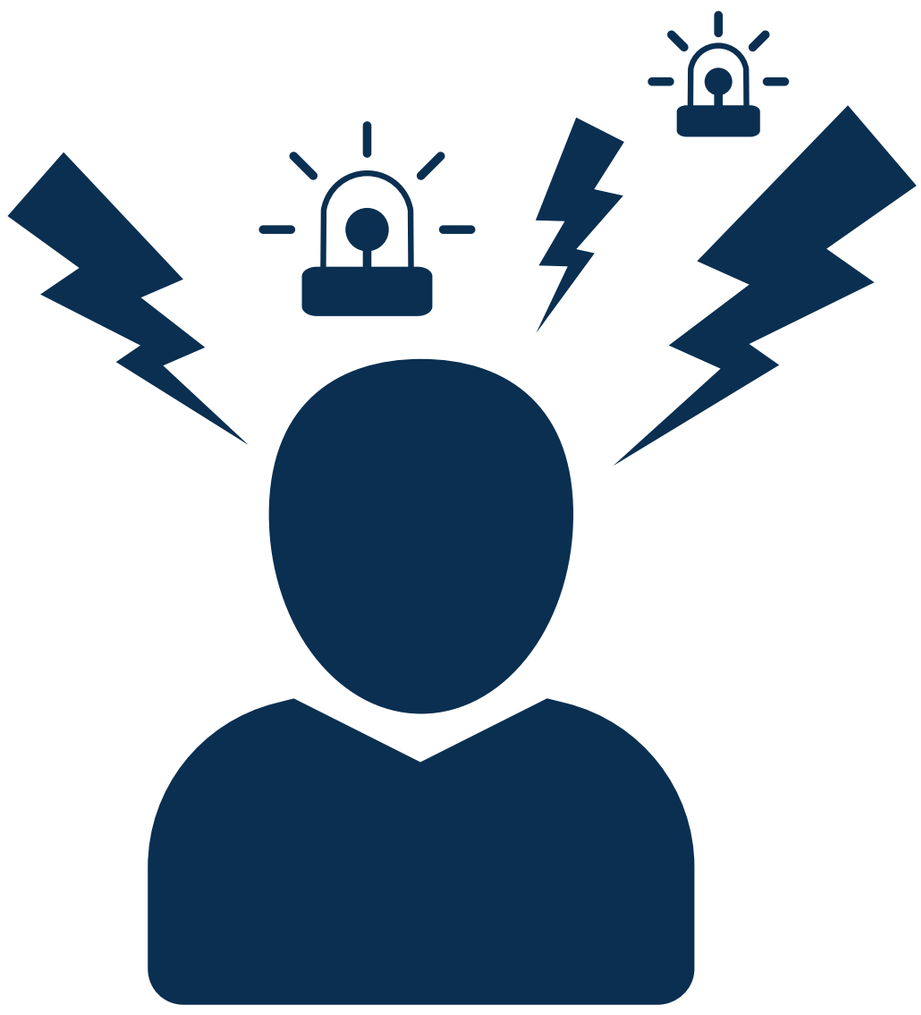
Vor allem per E-Mail, aber auch SMS, Messenger oder Soziale Medien: Die Täter melden sich unter falscher Identität und geben einen für Sie relevanten Anlass vor, einer betrügerischen Aufforderung nachzukommen. Komplexe Social-Engineering-Angriffe beginnen häufig mit einem Anruf.

Sie sind aufgefordert umgehend zu reagieren

Sie könnten aufgefordert werden, auf einer gefälschten Webseite oder etwa per E-Mail sensible Informationen preiszugeben – meist Passwörter und andere Zugangsdaten. Oder Sie sollen eine Datei öffnen, in der sich Schadprogramme verstecken, die den Tätern Zugriff auf Ihre Daten verschaffen. Das kann der Anhang einer E-Mail sein oder ein Download, für den Sie auf einen Link klicken sollen.

Deutsche Bank

Versetzt Sie eine E-Mail in Aufregung?



Worauf achten?

Werden Sie misstrauisch, wenn eine Nachricht Ihnen Sorge bereitet oder emotional stark bewegt.

Warum?

Cyber-Kriminelle bezwecken damit, dass Sie ihren Aufforderungen ohne Zögern nachkommen. Sie geben eilige Anliegen vor, drohen mit Konsequenzen, appellieren an Ihre Hilfsbereitschaft oder machen falsche Versprechen.

Was tun?

Stopp – klicken Sie nicht auf Anhänge oder Links! Ist die Mitteilung überhaupt plausibel? Können Sie sich der Identität des Absenders sicher sein? Mehr dazu in den folgenden Tipps.

Deutsche Bank

Können Sie dem Absender vertrauen?

Worauf achten?

Auch wenn die E-Mail von einem namhaften Unternehmen, einer seriösen Organisation oder bekannten Person zu stammen scheint, so könnte es sich um eine Fälschung handeln.

Warum?

Cyber-Kriminelle verwenden oftmals E-Mail-Adressen, die den echten zum Verwechseln ähnlich sind.

Was tun?

Prüfen Sie, ob die E-Mail-Adresse des Absenders wirklich stimmt. Achten Sie auf jeden Buchstaben und jedes Zeichen! Auch hinter einer privaten E-Mail-Adresse, die bei einem öffentlichen E-Mail-Anbieter angelegt wurde, könnten Betrüger stecken!

Deutsche Bank

Ist die Webseite echt?

Worauf achten?

Wie lautet die Internetadresse der Webseite, auf der Sie Daten eingeben sollen? Und wie die Internetadresse eines Downloads, den Sie anklicken sollen? Prüfen Sie, ob diese Adressen vertrauenswürdig sind.

Warum?

Vor allem gefälschte Log-in-Seiten sind von echten optisch oft nicht zu unterscheiden. Erst der Blick auf deren Internetadresse offenbart den Betrug. Auch der Link zu einem Download kann bösartige Absichten verraten.

Was tun?

Identifizieren Sie in der Internetadresse die genaue Zieladresse. Womöglich ist es nicht die des angeblichen Absenders. So geht‘s:

http(s)://hier-steht-was.Zieladresse.com/hier-auch

Starten Sie in der Internetadresse beim „//“ und suchen Sie den nächsten Slash. Springen Sie nach links über die Domain-Endung, beispielsweise „.com“, „.org“ oder „.de“, hinweg bis zum nächsten Punkt. Zwischen diesem und dem Slash rechts befindet sich die Zieladresse.

Deutsche Bank

Kennt der Absender persönliche Details?

Worauf achten?

Werden Sie in einer verdächtigen E-Mail persönlich angesprochen und nimmt sie Bezug zu privaten oder beruflichen Details, von denen nur wenige Menschen wissen können?

Warum?

Es könnte sich um den Angriff eines Social Engineers handeln, der Sie und Ihr Umfeld ausspioniert hat und sich als eine Person ausgibt, der Sie glauben.

Was tun?

Klicken Sie nicht auf Anhänge oder Links! Überprüfen Sie zunächst die E-Mail-Adresse. Setzen Sie sich beim geringsten Zweifel mit dem Absender in Verbindung. Nutzen Sie dazu Kontaktdaten aus anderer Quelle.

Deutsche Bank

Vorsicht vor gefährlichen Datei-Arten!

Worauf achten?

Sie sollen eine Word-, Excel- oder PowerPoint-Datei öffnen und werden dabei aufgefordert, Makros zu aktivieren? Oder sollen Sie ein Datenpaket mit der Endung „.zip“ oder ein Programm mit der Endung „.exe“ laden?

Warum?

Vorsicht: Diese Dateiarten werden von Cyber-Kriminellen genutzt, um Computer mit Schadprogrammen zu infizieren.

Was tun?

Aktivieren Sie in Office-Programmen niemals Makros und öffnen Sie keine Dateien mit den Endungen „.zip“ oder „.exe“, ohne sich von der Vertrauenswürdigkeit der Dateien überzeugt zu haben.

Deutsche Bank

Betrügerische Anrufe und SMS-Nachrichten

Nennen Sie am Telefon niemals Zugangsdaten!

Es könnte sich um Kriminelle handeln, die sich als Mitarbeiter eines IT-Supports, eines Kreditkarten-Unternehmens oder Ihrer Bank ausgeben und ein Sicherheitsproblem vorgeben. Seriöse Unternehmen werden Sie niemals darum bitten, am Telefon Passwörter für Ihre Online-Zugänge zu nennen.

Vorsicht vor betrügerischen SMS!

Betrüger versenden Textnachrichten im Namen von Banken und fordern wegen angeblicher Vorfälle dazu auf, Zugangsdaten auf einer gefälschten Webseite oder per Anruf bei einem gefälschten Callcenter preiszugeben.

Gut zu wissen

Installieren Sie Anti-Viren-Programme

Aktualisieren Sie diese Wächter regelmäßig. Hundertprozentigen Schutz bieten sie jedoch nicht!

Sorgen Sie regelmäßig für Back-ups

So können Sie Ihre Daten wiederherstellen, falls Sie Ziel eines Phishing-Angriffs geworden sind, bei dem ein Schadprogramm Ihre Daten verschlüsselt hat und Sie ein Lösegeld zahlen sollen.

Zeigt Ihr Smartphone Anzeichen einer Infektion?

Reagiert es langsamer, ist der Datenverbrauch gestiegen und der Akku schnell leer? Setzen Sie das Gerät zurück, installieren Sie Betriebssystem, Apps und Daten neu.

Impressum und Haftungsausschuss

Dieser private Leitfaden zur IT-Sicherheit dient nur zu Informationszwecken und ist für Ihren persönlichen Gebrauch bestimmt. Dieser Leitfaden und die allgemeine Beschreibung der Sicherheitsmaßnahmen sind nur illustrativ, sie stellen weder explizit noch implizit ein Angebot dar, so dass kein vertragliches oder außervertragliches Schuldverhältnis begründet wird oder eine vertragliche oder außervertragliche Haftung der Deutschen Bank AG, einer ihrer Filialen oder eines verbundenen Unternehmens daraus resultieren kann.

In Bezug auf die Genauigkeit, Vollständigkeit oder Zuverlässigkeit der Informationen des Leitfadens wird keine Zusicherung oder Garantie, weder ausdrücklich noch stillschweigend, gegeben, noch ist beabsichtigt, dass es sich um eine vollständige Erklärung oder Zusammenfassung aller Materialien zur Informationssicherheit handelt. Dieser Leitfaden basiert auf Informationen, die die Deutsche Bank zum Zeitpunkt der Erstellung dieses Dokuments für zuverlässig erachtet. Die in diesem Dokument enthaltene Annahmen, Schätzungen und Meinungen stellen unsere Bewertung zum Zeitpunkt der Erstellung des Dokuments dar und können ohne vorherige Ankündigung geändert werden. Die Deutsche Bank ist nicht verantwortlich für die Aktualisierung jeglicher hierin enthaltenen Informationen.

Die Deutsche Bank AG verfügt über eine Zulassung nach dem deutschen Kreditwesengesetz (zuständige Behörden: Europäische Zentralbank und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)) sowie im Vereinigten Königreich über eine Zulassung der Prudential Regulation Authority. Sie unterliegt der Aufsicht der Europäischen Zentralbank und der BaFin sowie im begrenzten Umfang der Prudential Regulation Authority und Financial Conduct Authority im Vereinigten Königreich. Einzelheiten zum Umfang der Zulassung und Aufsicht durch diese Behörden sind auf Anfrage erhältlich.

Dieser Private Guide wurde von der Deutsche Bank Gruppe genehmigt bzw. übermittelt. Die Bereitstellung von Produkten oder Dienstleistungen, auf die hierin Bezug genommen wird, durch die Deutsche Bank AG oder ihre Zweigniederlassungen bzw. verbundenen Unternehmen erfolgt nach den anwendbaren örtlichen Gesetzen und Vorschriften. Weitere Informationen unter: http://www.db.com