Keine Angst vorm Onlinebanking!

Referent: Patrick Kaufhold

Tel. 0172 7681664

E-Mail: pkaufhold@t-online.de

DIGITALPATEN HILDEN

Meine persönliche Erfahrung mit dem Online-Banking

- Onlinebanking betreibe ich seit ca. 1990. Anfangs über **BTX** in Verbindung mit einem Konto bei der Postbank.

  (Online-Banking über das **Internet** gibt es in Deutschland erst seit ca. 1995).

- Im Laufe der Jahre habe ich Online-Konten bei mehr als 20 verschiedenen Banken / Kreditinstituten geführt.
  (Giro-Konten, Wertpapierdepots, Tages- und Festgelder).

- **In über 30 Jahren Online-Banking bei diversen Banken habe ich nicht eine Unregelmäßigkeit erlebt.**

DIGITALPATEN HILDEN

Typische Bedenken älterer Menschen gegenüber dem Online-Banking

- **Sicherheitsbedenken:** Ältere Menschen sind oft vorsichtiger, wenn es um den Schutz ihrer persönlichen Daten und Finanzen geht. Sie können Bedenken hinsichtlich der Sicherheit von Online-Banking-Plattformen haben und befürchten, Opfer von Betrug oder Identitätsdiebstahl zu werden. Phishing-Angriffe und andere betrügerische Aktivitäten sind ebenfalls eine Sorge.

- **Technische Schwierigkeiten:** Viele ältere Menschen fühlen sich möglicherweise unsicher im Umgang mit neuen Technologien und haben Bedenken, dass sie mit den komplexen Funktionen von Online-Banking-Plattformen nicht zurechtkommen. Sie können Angst haben, etwas falsch zu machen oder versehentlich Fehler zu verursachen, die zu finanziellen Verlusten führen könnten.

- **Mangelndes Vertrauen:** Einige ältere Menschen haben möglicherweise generell weniger Vertrauen in Online-Dienste und fühlen sich wohler mit dem persönlichen Kontakt zu Bankmitarbeitern in einer Filiale. Sie bevorzugen den traditionellen Bankbesuch, um sich direkt mit einem Bankmitarbeiter austauschen zu können und Fragen zu klären.

- **Schwierigkeiten bei der Nutzung von Technologie:** Ältere Menschen können aufgrund von Seh- oder Motorikproblemen Schwierigkeiten haben, kleine Bildschirme oder winzige Tasten auf Smartphones oder Tablets zu bedienen. Dies kann ihre Frustration verstärken und ihre Bereitschaft zur Nutzung von Online-Banking-Diensten verringern.

- **Fehlender persönlicher Kontakt:** Viele ältere Menschen schätzen die persönliche Beratung und Unterstützung, die sie in einer Bankfiliale erhalten können. Sie möchten möglicherweise einen Bankmitarbeiter direkt ansprechen können, um Rat zu erhalten oder spezifische Fragen zu klären.

DIGITALPATEN HILDEN

Welche Vorteile bietet mir Onlinebanking von zu Hause im Vergleich zur Filiale?

- **Bequemlichkeit:** Online Banking ermöglicht es den Kunden, ihre Bankgeschäfte von überall aus durchzuführen, solange sie eine Internetverbindung haben. Es ist nicht mehr erforderlich, persönlich zur Bankfiliale zu gehen und in Warteschlangen zu stehen. Bankgeschäfte können bequem von zu Hause oder unterwegs erledigt werden.
- **Zeitersparnis:** Mit Online Banking sparen Kunden Zeit. Überweisungen, Kontostands-Abfragen, Rechnungszahlungen und andere Banktransaktionen können mit wenigen Klicks erledigt werden. Es ist nicht mehr nötig, Papierformulare auszufüllen oder ein SB-Terminal zu nutzen.
- **Rund-um-die-Uhr-Zugang:** Online Banking steht rund um die Uhr zur Verfügung. Kunden können jederzeit auf ihre Bankkonten zugreifen und Transaktionen durchführen, unabhängig von den Öffnungszeiten der Bankfilialen.
- **Übersicht und Kontrolle:** Durch Online Banking haben Kunden einen besseren Überblick über ihre Finanzen. Sie können ihre Kontostände in Echtzeit überprüfen, Transaktionshistorien einsehen und detaillierte Kontoauszüge herunterladen.
- **Automatisierte Funktionen:** Online Banking bietet verschiedene automatisierte Funktionen, die den Kunden das Leben erleichtern, z.B. das Einrichten von Überweisungsvorlagen oder das automatische Erkennen von Zahlungsempfängern.
- **Kostenersparnis:** Online-Konten sind oft günstiger als „herkömmliche Konten“, einige wenige sogar völlig kostenlos.

DIGITALPATEN HILDEN

Verbreitung von Online-Banking in Deutschland*

- Rund 56% der deutschen Bevölkerung nutzen Onlinebanking. Zum Vergleich: in Dänemark sind es 95%, in den Niederlanden 91%. In der EU belegt Deutschland damit den fünftletzten Platz.
- Anteil der 16-24-jährigen: 58%
- Anteil der 25-44-jährigen: 83%
- Anteil der 45-64-jährigen: 60%
- Anteil der über 65-jährigen: 31%

*Quelle: Statistisches Bundesamt, Erhebung der Daten im 1. Quartal 2020

DIGITALPATEN HILDEN

Voraussetzungen, um am Online-Banking teilzunehmen

- Ein handelsüblicher Computer, ein Smartphone oder ein Tablet.
- Ein Internetanschluss
- Internet-Browser (z.B. Firefox, Chrome, Safari, Edge) und/oder Banking-App Ihrer Bank
- Zugangs-Daten Ihrer Bank: Benutzernamen und Passwort
- Ein sicheres TAN-Verfahren (TAN = Transaktions-Nummer)

DIGITALPATEN HILDEN

Was ist eine TAN und wofür wird sie benötigt?

- TAN steht für "Transaktionsnummer" und ist eine Art Einmalpasswort, das für Online-Banking-Transaktionen verwendet wird. Die TAN dient als zusätzliche zwingend erforderliche Sicherheitsebene, um sicherzustellen, dass nur der rechtmäßige Kontoinhaber Transaktionen (Überweisungen, Einrichtung von Daueraufträgen, usw.) durchführen kann.
- Beim Onlinebanking brauchten Kunden immer schon eine PIN zum Einloggen und eine TAN als Code für die Überweisung. Mit einem geklauten Passwort allein konnten Betrüger also nie Geld vom Konto holen.
- Die TAN erfüllt somit die Funktion der sogenannten **Zwei-Faktor-Authentifizierung**. Ihr Konto wird nicht nur durch das Kennwort gesichert, sondern darüber hinaus durch die Abfrage einer TAN, also einem zufällig generierten Code. Mit der Eingabe dieser TAN stellen Sie den zweiten Faktor bereit und beweisen, dass Sie den Zugriff selbst autorisieren.
- Je nach Bank kommen unterschiedliche TAN-Verfahren zum Einsatz. Manche Banken bieten dem Kunden die Wahl zwischen verschiedenen TAN-Verfahren (Beispiel Sparkasse: Push-Tan-Verfahren oder ChipTAN-Verfahren), andere Banken geben ein bestimmtes TAN-Verfahren vor.

Welche TAN-Verfahren gibt es? (Seite 1 von 2)

- **TAN-Listen**

  Das früher gängige TAN-Verfahren. Eine Papier-Liste mit TAN-Nummern. Die Methode gilt als unsicher und darf seit dem 14.September 2019 nicht mehr im Zahlungsverkehr verwendet werden.

- **m-TAN** – die SMS aufs Handy

  Beim m-TAN-Verfahren wird die TAN per SMS aufs Handy geschickt. Das Verfahren gilt nur als relativ sicher (TAN könnte abgefangen werden) und wurde mittlerweile von den meisten Banken abgeschafft.

- **Push-TAN** (auch als **App-TAN** bezeichnet) - TAN wird per Handy-App generiert

  Im Unterschied zur mTAN nutzen Sie hier eine spezielle Smartphone-App, in der die TAN generiert wird. Das Verfahren gilt als sehr sicher. Insbesondere dann, wenn für Onlinebanking und App verschiedene Geräte verwendet werden.
  Beispiel: Onlinebanking am PC und Freigabe über das Smartphone.

Welche TAN-Verfahren gibt es? (Seite 2 von 2)

- **Chip-TAN**

  Beim Chip-TAN-Verfahren kommt ein TAN-Generator in Kombination mit dem Chip auf der Bankkarte zum Einsatz. Der Generator ermittelt durch Auslesen eines flackernden Feldes auf dem Schirm die jeweils erforderliche TAN. Mittlerweile gibt es auch das „Chip-TAN-QR“-Verfahren, bei dem ein QR-Code eingescannt wird. In der Bedienung ist dies schneller und komfortabler als das herkömmliche Chip-Tan-Verfahren.

  Beide Varianten bieten eine sehr hohe Sicherheit, da zwei getrennte Geräte verwendet werden und zusätzlich die Bankkarte nötig ist.

- **Photo-TAN**

  Bei manchen Banken kommt ein dem Chip-Tan-Verfahren ähnlicher TAN-Generator zum Einsatz, der sich Photo-TAN nennt. Hier wird der QR-Code mittels einer Photo-TAN-App auf dem Smartphone gescannt. Ebenfalls hohe Sicherheit ähnlich wie beim Push-TAN-Verfahren.

DIGITALPATEN HILDEN

Was kann ich selber tun, um das Online-Banking noch sicherer zu machen?

1. **Sichere Passwörter verwenden:** Verwenden Sie starke Passwörter, die eine Kombination aus Buchstaben, Zahlen und Sonderzeichen enthalten.

2. **Sichere Internetverbindung nutzen:** Vermeiden Sie die Nutzung von öffentlichen WLAN-Netzwerken, insbesondere beim Zugriff auf Ihr Online-Banking-Konto. Verwenden Sie stattdessen ein sicheres, passwortgeschütztes Netzwerk (z.B. ihr heimisches WLAN) oder eine mobile Datenverbindung.

3. **Aktuelle Sicherheitssoftware verwenden:** Stellen Sie sicher, dass Ihr Computer über eine aktuelle Antivirensoftware und eine Firewall verfügt. Halten Sie Ihr Betriebssystem und Ihre Programme auf dem neuesten Stand, um mögliche Sicherheitslücken zu schließen.

4. **Überprüfen Sie regelmäßig Ihre Kontobewegungen:** Überprüfen Sie Ihre Bankauszüge und Transaktionsverläufe regelmäßig, um ungewöhnliche Aktivitäten oder unbekannte Transaktionen zu identifizieren. Melden Sie verdächtige Aktivitäten sofort Ihrer Bank.

5. **Tageslimit festlegen:** Legen Sie ein Tageslimit für Überweisungen fest, um den Schaden im unwahrscheinlichen „Falle des Falles“ möglichst gering zu halten.

6. **Vorsicht bei Phishing-Versuchen:** Seien Sie vorsichtig bei E-Mails, Anrufen oder Textnachrichten, die angeblich von Ihrer Bank stammen. Geben Sie niemals vertrauliche Informationen preis, wenn Sie nicht 100% sicher sind, dass die Anfrage legitim ist. Überprüfen Sie bei Zweifeln die Echtheit von Kommunikationen, indem Sie direkt bei Ihrer Bank nachfragen.

DIGITALPATEN HILDEN

Was bedeutet Phishing?

Phishing (=Kunstwort aus „Password“ und „Fishing) ist eine Form des Internetbetrugs, bei der Angreifer betrügerische Techniken einsetzen, um persönliche Informationen, wie Benutzernamen, Passwörter, Kreditkartennummern oder andere sensible Daten von ahnungslosen Opfern zu stehlen. Die Täter geben sich dabei oft als vertrauenswürdige Quellen aus, wie beispielsweise Banken, soziale Netzwerke, E-Mail-Dienste oder andere Online-Dienstleister.

Die gängigste Methode beim Phishing ist das Versenden gefälschter E-Mails, die wie legitime Nachrichten aussehen. Diese E-Mails enthalten oft Links zu gefälschten Websites, die den echten Websites sehr ähnlich sehen, tatsächlich aber von den Angreifern kontrolliert werden. Sobald ein Opfer auf den Link klickt und seine Daten auf der gefälschten Website eingibt, werden diese an die Angreifer übermittelt.

Phishing kann auch über andere Kanäle wie SMS (Smishing), Telefonanrufe (Vishing) oder soziale Medien stattfinden. Die Absicht der Angreifer ist es, persönliche Daten zu stehlen, um Identitätsdiebstahl zu betreiben, finanziellen Schaden anzurichten oder andere betrügerische Aktivitäten durchzuführen.

Um sich vor Phishing-Angriffen zu schützen, ist es wichtig, misstrauisch gegenüber verdächtigen E-Mails, Nachrichten oder Telefonanrufen zu sein. Man sollte niemals persönliche Informationen preisgeben oder auf Links in solchen Nachrichten klicken, es sei denn, man ist sich absolut sicher, dass sie von einer vertrauenswürdigen Quelle stammen.

DIGITALPATEN HILDEN

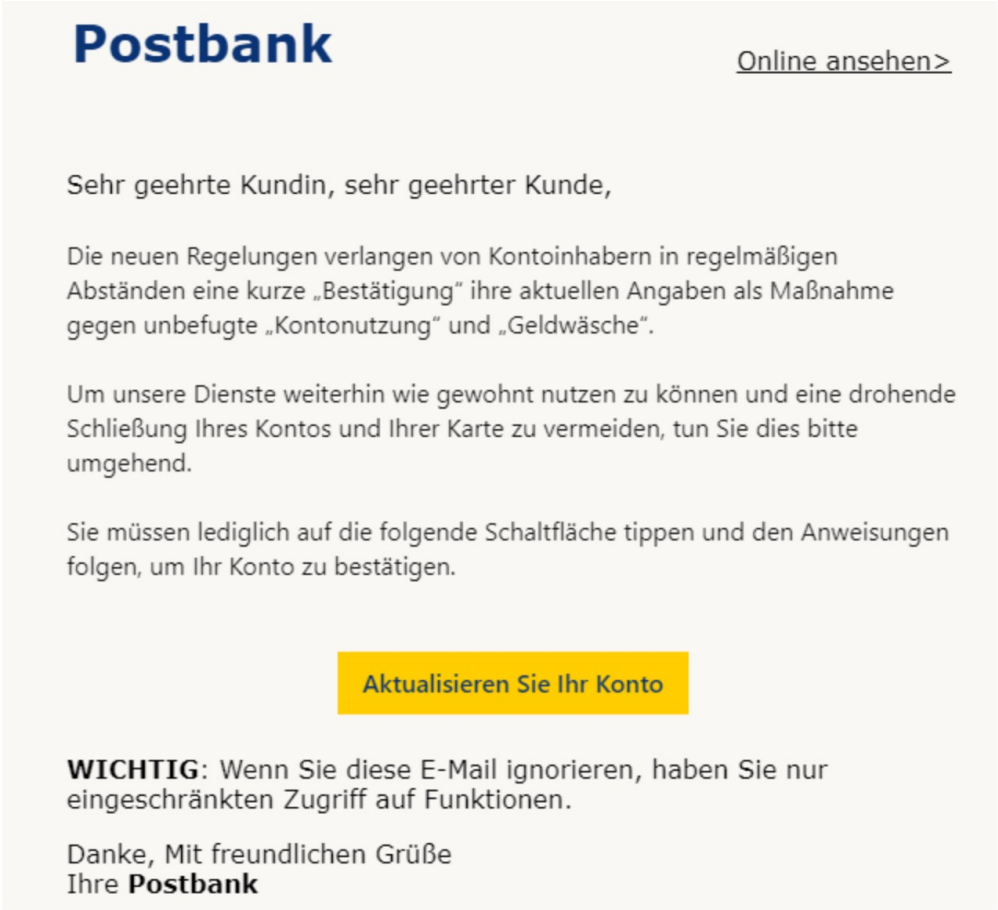
Woran erkenne ich Phishing-Mails?

- Fehlende Absenderangaben und/oder Verwendung eines ähnlich klingenden Domännamens.
  Beispiel: service@ihre-bankk.com anstatt service@ihre-bank.com
- Sprache und Rechtschreibung: Phishing-E-Mails enthalten oft Rechtschreib- und Grammatikfehler.
- Dringende Aufforderungen: Phisher versuchen oft, Sie unter Druck zu setzen, indem sie behaupten, dass Ihr Konto gefährdet ist, gesperrt wird, oder dass Sie sofort handeln müssen.
- Fehlende persönliche Ansprache: E-Mails von echten Banken verwenden normalerweise Ihren vollen Namen, während Phishing-E-Mails allgemeine Begrüßungen wie "Sehr geehrter Kunde" verwenden.
- Persönliche Informationen: Seriöse Banken fragen niemals nach sensiblen persönlichen Informationen oder Passwörtern per E-Mail.
- Aufforderung, Anhänge oder Links anzuklicken.

DIGITALPATEN HILDEN

Phishing-Mail

Beispiel 1



Postbank

Online ansehen>

Sehr geehrte Kundin, sehr geehrter Kunde,

Die neuen Regelungen verlangen von Kontoinhabern in regelmäßigen Abständen eine kurze „Bestätigung" ihre aktuellen Angaben als Maßnahme gegen unbefugte „Kontonutzung" und „Geldwäsche".

Um unsere Dienste weiterhin wie gewohnt nutzen zu können und eine drohende Schließung Ihres Kontos und Ihrer Karte zu vermeiden, tun Sie dies bitte umgehend.

Sie müssen lediglich auf die folgende Schaltfläche tippen und den Anweisungen folgen, um Ihr Konto zu bestätigen.

Aktualisieren Sie Ihr Konto

WICHTIG: Wenn Sie diese E-Mail ignorieren, haben Sie nur eingeschränkten Zugriff auf Funktionen.

Danke, Mit freundlichen Grüße
Ihre **Postbank**

Phishing-Mail

Beispiel 1

Postbank 1 6 Online ansehen>

Sehr geehrte Kundin, sehr geehrter Kunde, 2

Die neuen Regelungen verlangen von Kontoinhabern in regelmäßigen Abständen eine kurze „Bestätigung" ihre aktuellen Angaben als Maßnahme 3 gegen unbefugte „Kontonutzung" und „Geldwäsche".

Um unsere Dienste weiterhin wie gewohnt nutzen zu können und eine drohende Schließung Ihres Kontos und Ihrer Karte zu vermeiden, tun Sie dies bitte 4 umgehend. 5

Sie müssen lediglich auf die folgende Schaltfläche tippen und den Anweisungen folgen, um Ihr Konto zu bestätigen.

Aktualisieren Sie Ihr Konto 6

WICHTIG: Wenn Sie diese E-Mail ignorieren, haben Sie nur eingeschränkten Zugriff auf Funktionen. 4

Danke, Mit freundlichen Grüße 3
Ihre **Postbank** 1

Woran erkenne ich, dass es sich um eine Phishing-Mail handelt?

1 Fehlende bzw. ungenaue Absenderangabe

2 Keine persönliche Anrede

3 Grammatikfehler

4 Drohung mit der Sperrung des Kontos, oder zumindest damit, dass das Konto nur noch eingeschränkt zur Verfügung stehen wird.

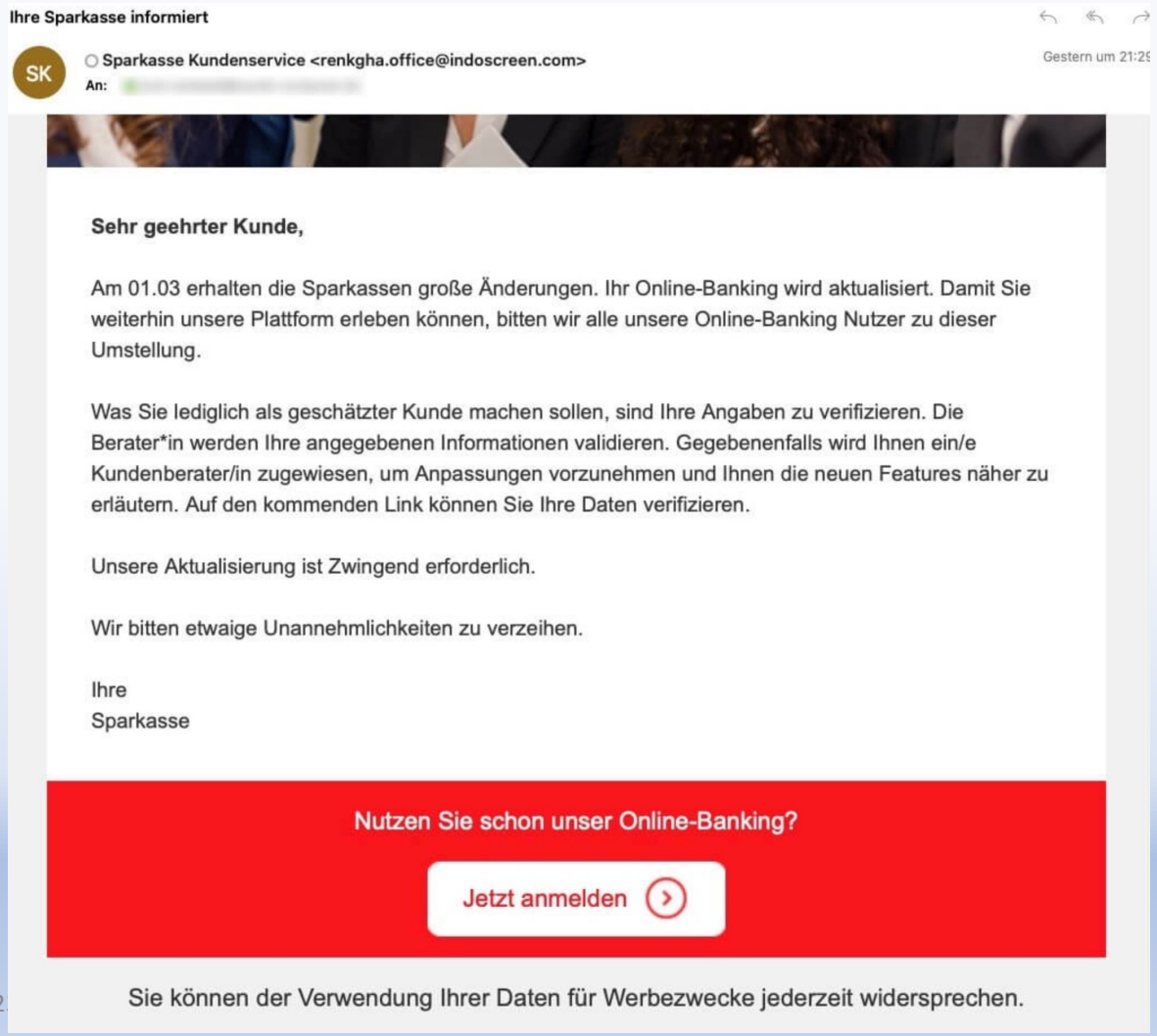
5 Es wird zeitlicher Druck aufgebaut.

6 Die Aufforderung, auf einen Link zu klicken

DIGITALPATEN HILDEN

Phishing-Mail

Beispiel 2



Ihre Sparkasse informiert

SK

Sparkasse Kundenservice <renkgha.office@indoscreen.com>

An:

Gestern um 21:2

Sehr geehrter Kunde,

Am 01.03 erhalten die Sparkassen große Änderungen. Ihr Online-Banking wird aktualisiert. Damit Sie weiterhin unsere Plattform erleben können, bitten wir alle unsere Online-Banking Nutzer zu dieser Umstellung.

Was Sie lediglich als geschätzter Kunde machen sollen, sind Ihre Angaben zu verifizieren. Die Berater*in werden Ihre angegebenen Informationen validieren. Gegebenenfalls wird Ihnen ein/e Kundenberater/in zugewiesen, um Anpassungen vorzunehmen und Ihnen die neuen Features näher zu erläutern. Auf den kommenden Link können Sie Ihre Daten verifizieren.

Unsere Aktualisierung ist Zwingend erforderlich.

Wir bitten etwaige Unannehmlichkeiten zu verzeihen.

Ihre
Sparkasse

Nutzen Sie schon unser Online-Banking?

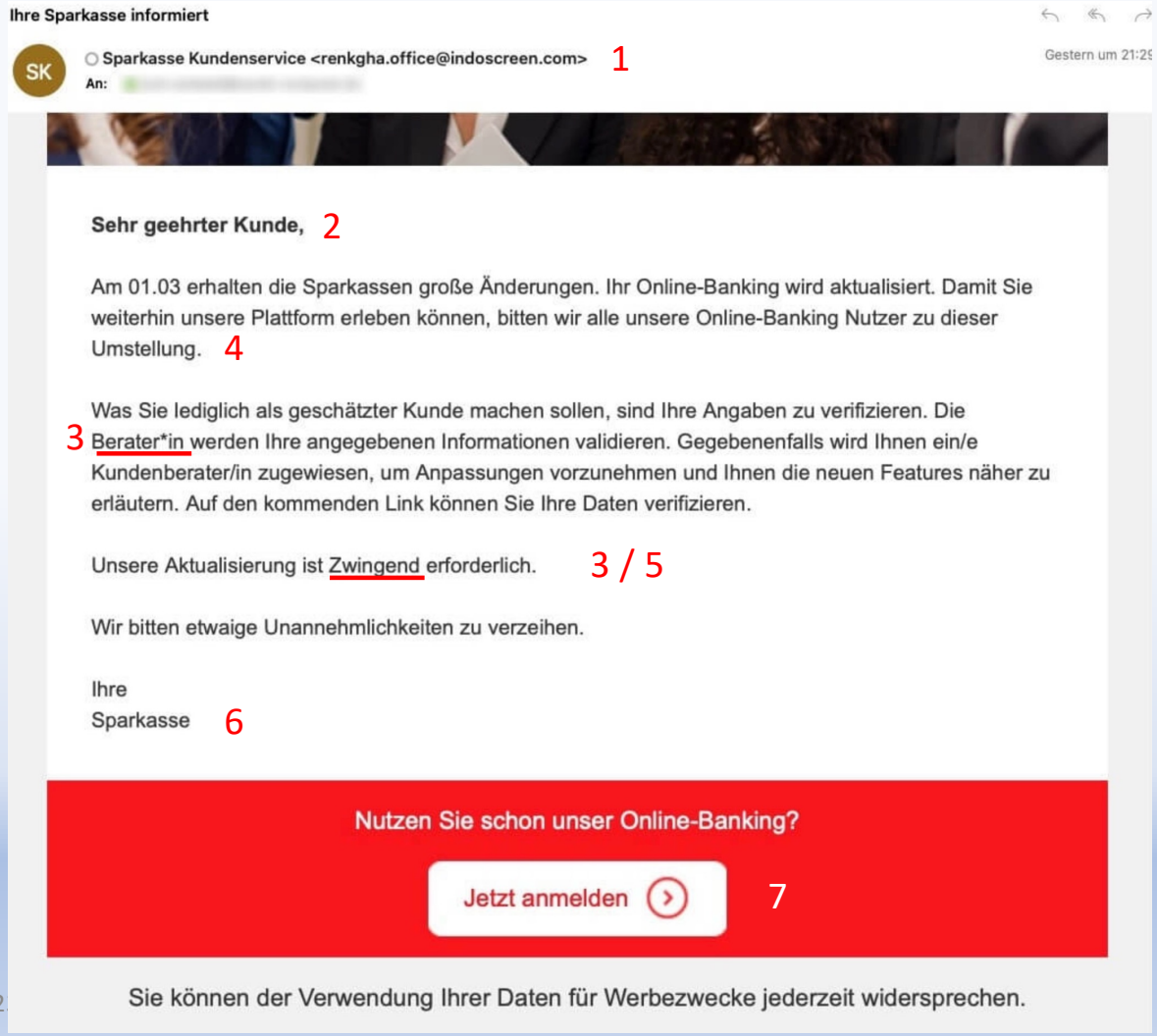
Jetzt anmelden

Sie können der Verwendung Ihrer Daten für Werbezwecke jederzeit widersprechen.

DIGITALPATEN HILDEN

Phishing-Mail

Beispiel 2



Ihre Sparkasse informiert

SK Sparkasse Kundenservice <renkgha.office@indoscreen.com> 1

An:

Gestern um 21:2

Sehr geehrter Kunde, 2

Am 01.03 erhalten die Sparkassen große Änderungen. Ihr Online-Banking wird aktualisiert. Damit Sie weiterhin unsere Plattform erleben können, bitten wir alle unsere Online-Banking Nutzer zu dieser Umstellung. 4

3 Berater*in werden Ihre angegebenen Informationen validieren. Gegebenenfalls wird Ihnen ein/e Kundenberater/in zugewiesen, um Anpassungen vorzunehmen und Ihnen die neuen Features näher zu erläutern. Auf den kommenden Link können Sie Ihre Daten verifizieren.

Unsere Aktualisierung ist Zwingend erforderlich. 3 / 5

Wir bitten etwaige Unannehmlichkeiten zu verzeihen.

Ihre
Sparkasse 6

Nutzen Sie schon unser Online-Banking?

Jetzt anmelden 7

Sie können der Verwendung Ihrer Daten für Werbezwecke jederzeit widersprechen.

Woran erkenne ich, dass es sich um eine Phishing-Mail handelt?

1 Der Alias (Sparkasse Kundenservice) scheint echt zu sein, aber die E-Mail-Adresse stammt von einer anderen Domain.

2 Keine persönliche Anrede

3 Grammatikfehler / Rechtschreibefehler

4 Indirekte Drohung, dass das Konto online nicht mehr zur Verfügung stehen wird, wenn man der Aufforderung nicht Folge leistet.

5 Es wird (indirekt) Druck aufgebaut.

6 Ungenauer Absender

7 Die Aufforderung, auf einen Link zu klicken

DIGITALPATEN HILDEN

Wie schütze ich mich vor Phishing-Mails?

- Seien Sie misstrauisch gegenüber E-Mails, die unerwartet kommen oder dringende Handlungen erfordern. Phishing-E-Mails verwenden oft Angst oder Neugier, um Sie zum Klicken auf Links oder Öffnen von Anhängen zu bewegen.
- Klicken Sie nicht auf Links in verdächtigen E-Mails, insbesondere wenn sie zu einer Anmeldeseite führen. Wenn Sie sich in Ihrem Bankkonto einloggen, geben Sie die URL manuell in Ihren Browser ein, oder verwenden Sie ein Lesezeichen.
- Öffnen Sie niemals Anhänge einer E-Mail, die Ihnen verdächtig erscheint!
- Gefälschte Nachrichten und Webseiten sind oft sehr professionell und individualisiert gestaltet. Lassen Sie sich dadurch aber nicht täuschen: **Ihre Bank fordert Sie niemals dazu auf, vertrauliche Daten wie PIN, TAN oder Kontonummer bekannt zu geben.**
- Wenn Sie eine verdächtige Phishing-E-Mail erhalten, melden Sie diese Ihrer Bank, damit diese Maßnahmen ergreifen kann, um andere Benutzer zu schützen.
- Löschen Sie die Phishing-Mail oder schieben Sie sie in Ihren Spam-Ordner.

Zusammenfassung und Fazit

- Online-Banking ist bequem und bietet viele Vorteile.
- Mit den aktuell von den meisten Banken eingesetzten TAN-Verfahren und der damit verbundenen Zwei-Faktor-Authentifizierung ist eine sehr große Sicherheit beim Online-Banking gewährleistet. Dass es Hackern gelingt, in der **direkten Kommunikation zwischen Bank und Kunden** Daten abzugreifen und das Konto zu plündern, ist extrem unwahrscheinlich.
- Aber: es gibt - wie fast immer im Leben - keine 100%ige Sicherheit. Kommt es zu Betrügereien beim Onlinebanking sind diese so gut wie immer durch unbedarftes oder fahrlässiges Verhalten der Nutzer begründet. Beispielsweise, indem man Bankgeschäfte in einem frei zugänglichen ungesicherten Netzwerk tätigt, telefonisch eine TAN-Nummer weitergibt, Zugangsdaten zum Online-Banking offen herum liegen lässt oder auf einen Link in einer Phishing-Mail klickt.