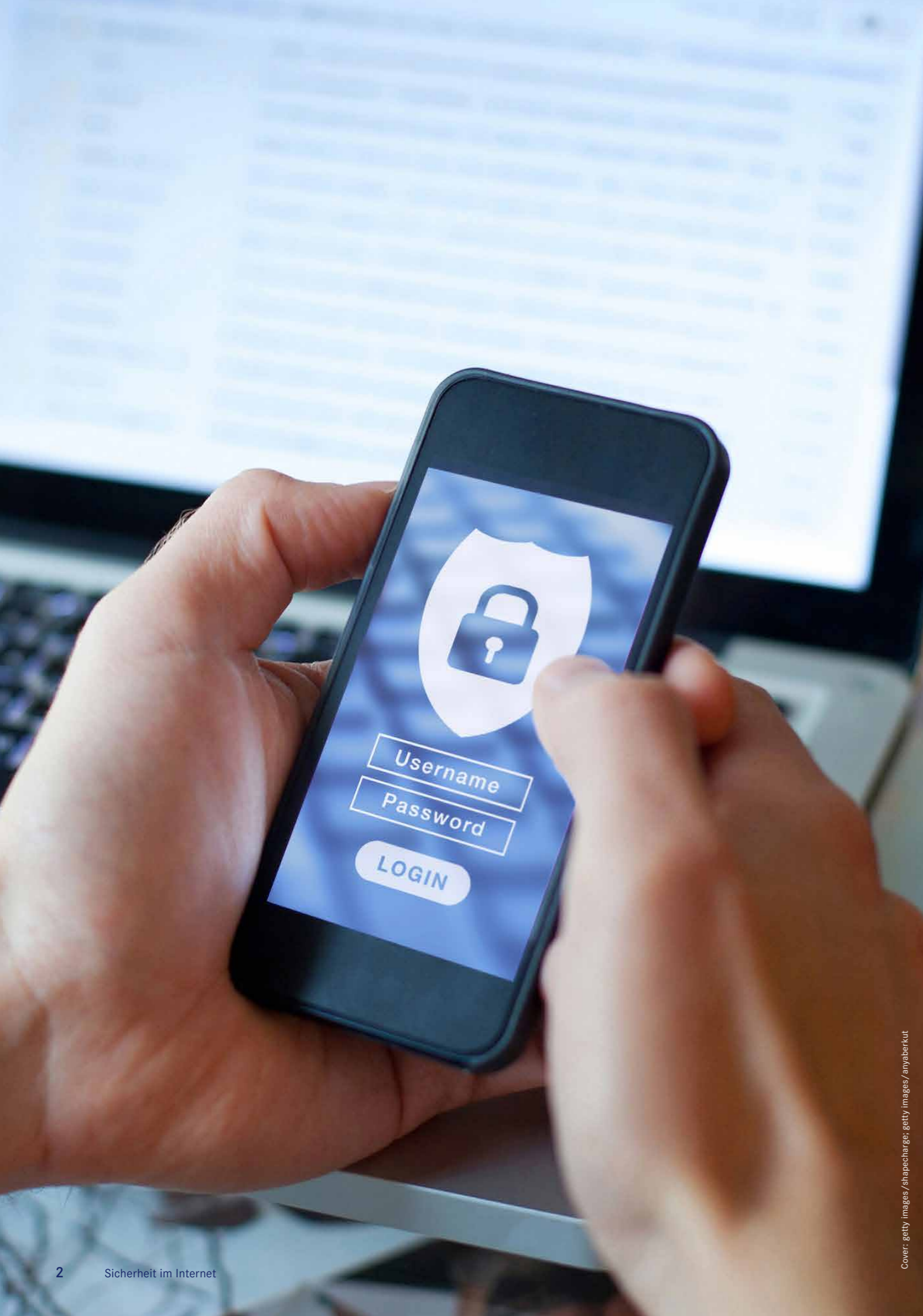




Alles im Blick?

Tipps und Tricks für Ihre
Sicherheit im Internet.



Cover: getty images / shapecharge, getty images / anyaberkut

Inhalt & Vorwort

4 Soziale Medien: Zwischen Vernetzung, Interaktion und Gefahren

- 4 Was sind soziale Medien?
- 4 Risiken und Herausforderungen im Umgang mit sozialen Medien
- 4 Desinformation & Manipulation
- 5 Datenschutz & Privatsphäre

6 Manipulation als Methode: Wie Social Engineering Phishing so erfolgreich macht

- 6 Was ist Social Engineering?
- 6 Wie funktioniert Social Engineering?
- 6 Phishing – das Angeln nach Daten
- 6 Phishing per E-Mail
- 9 Phishing per Post
- 9 Smishing
- 9 Anrufe mit falscher Identität („Vishing“)
- 9 Phishing über Suchmaschinen
- 10 Manipulation von sozialen Medien
- 10 Identitätsdiebstahl: Eine unterschätzte Gefahr
- 11 Empfehlungen für einen sicheren Umgang mit Online-Banking

12 Notfall-Telefonnummern bei Verlust Ihrer Debitkarte oder Kreditkarte

- 12 Debitkarte
- 12 Kreditkarten der apoBank

Liebe Leserinnen und Leser,

in der heutigen, digitalisierten Welt sind Themen wie Online-Sicherheit und Datenschutz von essentieller Bedeutung. Auch bei Verwendung von technischen Sicherheitsmaßnahmen, wie Verschlüsselung und Einsatz von sicheren Login-Mechanismen, bleibt dabei ein Risikofaktor immer bestehen, und der wird leider oft unzureichend beachtet: der Mensch.

Besonders im Bereich des Online-Bankings und der digitalen Kommunikation sehen sich Nutzerinnen und Nutzer immer häufiger gezielten Angriffen ausgesetzt. Methoden wie Social Engineering und Phishing setzen dabei auf das Vertrauen, die Hilfsbereitschaft oder die Unachtsamkeit im stressigen Alltag von Menschen, um an sensible persönliche, darunter vor allem finanziell bedeutsame Daten sowie Zugang zu geschützten Systemen zu gelangen.

Diese Broschüre möchte Ihnen dabei helfen, Betrugsversuche besser zu erkennen, und sich effektiv davor zu schützen. Sie bietet praxisnahe Informationen und konkrete Handlungsempfehlungen, damit Sie sicher und selbstbewusst im digitalen Umfeld unterwegs sein können – sei es beim Online-Banking, im E-Mail-Verkehr oder in sozialen Netzwerken.

Unser Ziel ist es, Sie zu sensibilisieren, ohne zu verunsichern, und Ihnen das notwendige Wissen an die Hand zu geben. Wir hoffen, Ihnen mit den nachfolgenden Tipps und Anregungen eine höhere Sicherheit Ihrer Daten sowie Informationen und damit Ihrer Identität in der digitalen Welt ermöglichen zu können.

Herzlichst

Marcel Breuer

Ihr Marcel Breuer

Informationssicherheitsbeauftragter der apoBank

1 Soziale Medien: Zwischen Vernetzung, Interaktion und Gefahren

Soziale Medien sind zu einem zentralen Bestandteil unseres Lebens geworden – privat wie beruflich. Plattformen wie Instagram, WhatsApp & Co. vernetzen Menschen weltweit.

Was sind soziale Medien?

Unter **sozialen Medien** versteht man digitale Plattformen, auf denen Nutzer Inhalte erstellen sowie teilen und miteinander interagieren können. Die sozialen Medien sind ein Raum für Information, Unterhaltung und Meinungsaustausch.

Zu den bekanntesten Plattformen zählen:

- f Facebook & Instagram**
für persönliche Netzwerke, Lifestyle und visuelle Inhalte
- in LinkedIn**
für berufliches Networking und Fachinhalte
- 🎵 TikTok**
für kreative Kurzvideos, Trends und Popkultur
- X (Twitter)**
für Nachrichten, Debatten und Echtzeitkommunikation
- 📱 WhatsApp**
für Nachrichten, Bilder, Sprachnachrichten und Videos

Risiken und Herausforderungen im Umgang mit sozialen Medien

Das Teilen von persönlichen Informationen, wie z. B. Fotos, Videos, Aufenthaltsorte, Geburtstage, berufliche Erfolge und Erlebnisse, birgt auch Gefahren: Die Daten können etwa in die Hände von Betrügern gelangen, die diese Informationen sammeln und gezielt ausnutzen, um Vertrauen zu ihren ausgewählten Opfern aufzubauen und diese zu täuschen.

Desinformation & Manipulation

Falschnachrichten, also bewusst erfundene oder verzerrte Meldungen, verbreiten sich schnell – oft schneller als seriöse Informationen. Algorithmen bevorzugen Inhalte, die emotionalisieren, nicht unbedingt solche, die aufklären. Zu Desinformation und Manipulation tragen auch generierte Kommentare bei, die gezielt bestimmte Meinungen verstärken und Angst verbreiten.



Datenschutz & Privatsphäre

Wer postet, hinterlässt Spuren. Viele Nutzer unterschätzen, in welchem Umfang und in welchem Detailgrad persönliche Informationen öffentlich sichtbar sind – und von Dritten ausgewertet werden. Prüfen Sie daher, ob Ihr Profil wirklich öffentlich zugänglich sein muss oder ob Sie es auf privat umstellen können. Nur wenn es privat ist, haben Sie die Kontrolle darüber, wer Ihre Daten sieht. Doch auch hier ist noch Vorsicht geboten: Gewähren Sie bitte nur Ihnen bekannten Personen Zugang zu Ihrem privaten Profil!

Das beschleunigte Wachstum von künstlicher Intelligenz (KI) kann ebenfalls Sicherheitsrisiken erhöhen. Denn aus öffentlich zugänglichen Informationen kann KI sehr schnell ein genaues Profil einer Person erstellen. Diese Informationen werden anschließend von Betrügern verwendet, um Vertrauen zu ihren Opfern aufzubauen und die psychischen Schwachstellen eines jeden vor allem mittels Angst und Zeitdruck für ihre Zwecke zu nutzen.



2 Manipulation als Methode: Wie Social Engineering Phishing so erfolgreich macht

getty images/Pexic

Was ist Social Engineering?

Social Engineering beschreibt Methoden, mit denen Täter gezielt versuchen, durch psychologische Manipulation an sensible Informationen und Zugänge zu gelangen. Dabei nutzen sie typischerweise Vertrauen, Hilfsbereitschaft sowie Unkenntnis aus und erzeugen Angst sowie Zeitdruck bei ihren Opfern. Die Täter setzen hier auf gut vorbereitete Muster und Drehbücher, um das Vertrauen der Opfer zu gewinnen und diese schrittweise zu manipulieren.

Bei dieser Vorgehensweise wird also auf die Schwachstelle Mensch abgezielt, sodass keine Notwendigkeit dafür besteht, aufwändig technische Barrieren oder Schutzmaßnahmen, wie z. B. Firewalls, zu umgehen.

Wie funktioniert Social Engineering?

Social Engineering kann auf vielen Wegen erfolgen. Die Angriffe wirken oft alltäglich oder harmlos, weil sie über vertraute Kommunikationskanäle stattfinden – wie E-Mail, Telefon, Brief oder soziale Netzwerke. Gerade deshalb ist es wichtig, die typischen Methoden und Merkmale zu kennen. Social Engineering nutzt dabei insbesondere menschliche Schwächen aus: Die Betrüger versuchen Vertrauen aufzubauen, die Emotionen von Menschen auszunutzen und Hilfsbereitschaft sowie stressige Situationen durch gezielte Ansprache für ihre betrügerischen Zwecke zu missbrauchen.

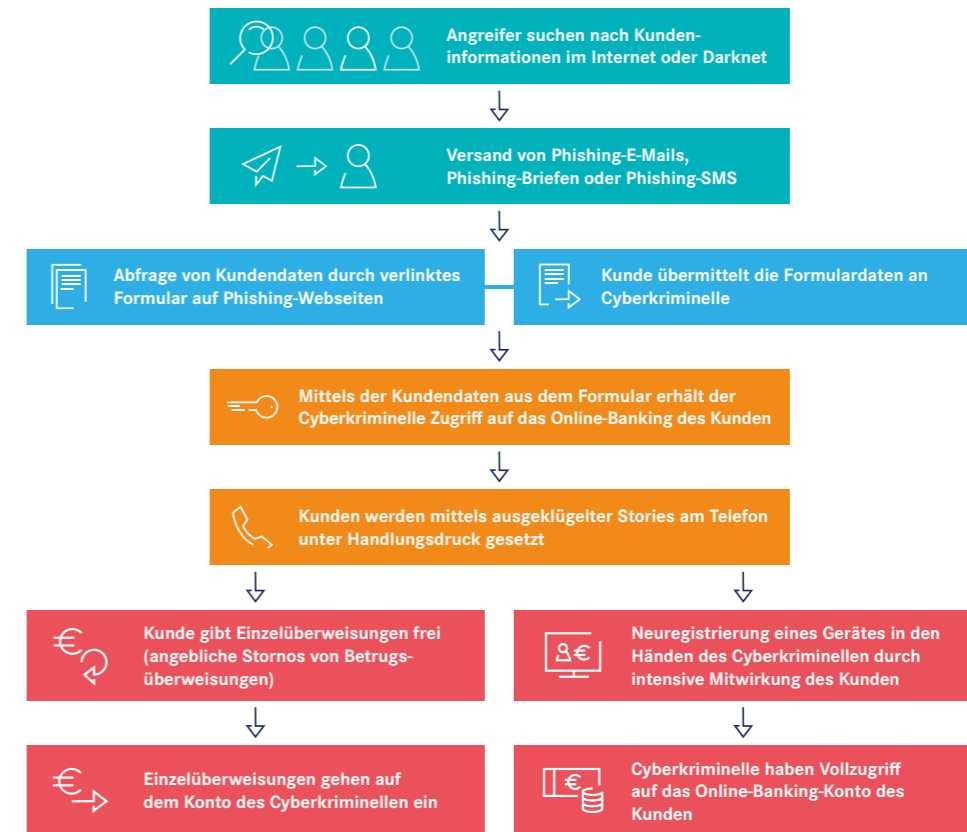
Phishing – das Angeln nach Daten

Phishing ist eine der bekanntesten und am weitesten verbreiteten Social-Engineering-Techniken. Über unterschiedliche Kanäle, wie E-Mail, Telefon, Post, SMS oder soziale Medien, werden die Opfer mit dem Ziel kontaktiert, dass sie möglichst viele sensible Informationen preisgeben. Oft werden die Kanäle in zeitlicher Abfolge miteinander kombiniert und sind aufeinander aufbauend eingesetzt.

Phishing per E-Mail

Betrüger versenden gefälschte E-Mails, die einen offiziellen und vertrauenswürdigen Charakter besitzen und vortäuschen, von Ihrer Bank oder einem Ihnen vertrauten Unternehmen zu stammen. Oft werden Sie dazu aufgefordert, in die E-Mails integrierten Links zu folgen, QR-Codes abzuscannen oder schädliche Anhänge zu öffnen. Bei den meist täuschend echt nachgemachten Zielseiten, auf die solche Links führen, handelt es sich um Fälschungen, die lediglich dem Ausspionieren Ihrer sensiblen Daten, wie Kreditkarteninformationen, Zugangsdaten (zum Online-Banking), Telefonnummern oder Kontakte, gelten. Für schadhafte Anhänge gilt: Hier können ebenfalls Informationen ausspioniert werden, nur bekommen Sie dies meist gar nicht mit. Der unlautere Informationstransfer geschieht beispielsweise, indem Bildschirmaktivitäten überwacht werden, Zugangsdaten und Passwörter mitgeschnitten werden oder auf Fotos, Dokumente und Kontakte zugegriffen wird. Darüber hinaus ist auch eine Fernsteuerung des Geräts möglich. Mit ihrer Hilfe können Nachrichten verschickt, Daten kopiert und weitere Aktionen ausgeführt werden.

Ablauf eines Phishing-Angriffs



Bei unerwarteten E-Mails ist daher besondere Aufmerksamkeit auf die Absenderadresse, enthaltene Links und Manipulationsversuche, etwa mittels Angst und Zeitdruck, zu richten.

Um Links zu überprüfen, empfiehlt sich das sog. Mouseover, das heißt man geht mit dem Cursor über eine Linktextstelle oder Adresse, ohne sie anzuklicken, und bekommt dadurch den tatsächlichen Link hinter dem Text in einem aufploppenden gelben Fensterchen angezeigt. Damit lassen sich oft der Absender oder das Ziel des Links identifizieren.

Achten Sie vor allem auf den korrekten Aufbau des Links:

<https://banking.apobank.de/auth/ui/app/auth/flow/apo-afp/password>



Entspricht die 2nd-Level-Domain in Kombination mit der Top-Level-Domain nicht der Ihnen bekannten Adresse, so kontaktieren Sie bitte Ihren zuständigen Berater bei der apoBank und fragen Sie nach.

Schützen Sie sich,
indem Sie die acht
As des Phishings
beachten:

1

Anrede

Nutzung einer unpersönlichen Anrede (ohne Namen)

„Sehr geehrter Kunde“
„Sehr geehrte Kundin, sehr geehrter Kunde“
„Guten Tag“

2

Absender

Es wird eine dringende Handlung vorgetäuscht

„Die Frist zur Durchführung endet am 25. Juni 2026. Nach Ablauf ist keine digitale Nutzung mehr möglich. Ihr Zugang wird gesperrt und der Zahlungsverkehr wird unterbrochen.“

3

Auffälligkeiten

Sind Formatierungsfehler oder Rechtschreibfehler erkennbar?

„Wir haben festgestellt, dass ihr ApoBank_Account gesperrt ist.“
„Sehr geehrtenu Damen und Herren,“

4

Anhänge

Beigefügte Anhänge können Schadsoftware enthalten,
die sich auf dem Computer/Smartphone installiert, sobald
auf ebenjene Anhänge geklickt wird.

5

Anklicken

**Links in E-Mails sind vor dem Anklicken mit dem sogenannten
Mouseover zu prüfen.** Führt der dem Text hinterlegte Link tatsächlich zu
einer Seite der apoBank? Falls nicht, kontaktieren Sie bitte Ihren Berater.

6

Aufforderung

Es wird eine dringende Handlung vorgetäuscht.

„Die Frist zur Durchführung endet am 25. Juni 2026. Nach Ablauf ist keine digitale Nutzung mehr möglich. Ihr Zugang wird gesperrt und der Zahlungsverkehr wird unterbrochen.“

7

Angst

Es wird ein Gefühl von Angst und Druck erzeugt.

„Betreff: Vorübergehende Sperrung! Ihr Konto wird in 5 Tagen gelöscht,
falls Sie keine Aktualisierung durchführen. Bitte klicken Sie auf den
Link, um Ihre Daten jetzt zu aktualisieren und den Zugang zu behalten.“

8

Aktualisierung

Es wird eine Aktualisierung vorgetäuscht.

„Wichtige Systemaktualisierung – Unverzögliche Reaktion notwendig“
„Unverzichtbare Sicherheitsaktualisierung – Ihr Handeln ist erforderlich“

Phishing per Post

Ähnlich dem E-Mail-Phishing wird von Betrügern auch der Postkanal genutzt, um an Ihre sensiblen Informationen zu gelangen: Betrüger versuchen, durch nachgeahmte offizielle Bankdokumente zu aktuellen Themen, wie neuen Sicherheitsmaßnahmen oder auch der Umsetzung neuer regulatorischer Vorgaben, Vertrauen zu erwecken und über QR-Codes (ähnlich dem Klicken auf einen Link) das Aufrufen einer gefälschten Zielwebseite zu provozieren. Die gefälschte Webseite dient nun wieder dazu, persönliche Informationen, wie Zugangsdaten, Kartendaten oder Kontaktinformationen, zu erhalten.

Smishing

Smishing ist ein weiterer Kanal, der von Betrügern genutzt wird. Hier geht es darum, Sie durch falsche SMS-Nachrichten dazu zu bringen, auf einen Link zu klicken und persönliche Daten preiszugeben. Der Begriff setzt sich zusammen aus „SMS“ und „Phishing“.

Folgen Sie keinen Links aus unerwarteten und nicht verifizierbaren Nachrichten – prüfen Sie die Echtheit über bekannte, offizielle Kontaktwege.

Anrufe mit falscher Identität („Vishing“)

Am Telefon geben sich Betrüger als Mitarbeitende Ihrer Bank aus und berichten von angeblich verdächtigen Buchungen, notwendigen Aktualisierungen im Online-Banking oder Sicherheitsprüfungen. Dabei setzen die Betrüger Sie häufig unter emotionalen und zeitlichen Druck – es sei dringend, man müsse sofort handeln, sonst drohten Konsequenzen. Deren Ziel ist es, Sie zur Herausgabe sensibler Informationen, wie Aktivierungscodes und Zugangsdaten, oder zur Durchführung bestimmter Handlungen, wie z. B. der Installation von Software oder der Durchführung von Änderungen in Ihrem Online-Banking (Limitänderungen/Registrierung eines neuen Gerätes etc.), zu bewegen.

Bitte beachten Sie hier auch: Rufnummern können gefälscht sein. Indem der Betrüger eine beliebige, häufig Ihnen bekannte und als vertrauenswürdig angesehene Rufnummer anzeigt und die echte Nummer versteckt, will er seine Identität verschleiern



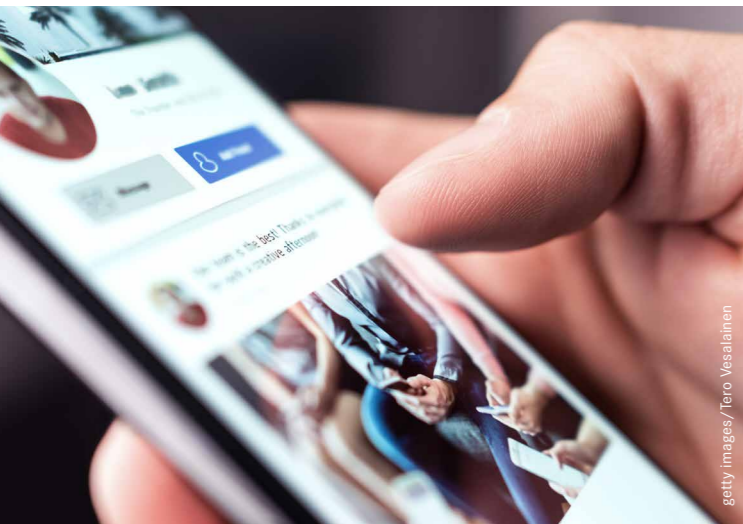
und Ihr Vertrauen erschleichen. Stimmen können zudem mittels künstlicher Intelligenz gefälscht werden, sodass eine Unterscheidung zu bekannten Stimmen sehr schwerfällt.

Seien Sie daher bei unerwarteten Anrufen und/oder Rückfragen bitte vorsichtig mit der Informationsweitergabe.

Phishing über Suchmaschinen

Betrüger leiten Sie hier in Telefonaten gezielt zu bestimmten Suchmaschinen, wie Google oder Bing, und geben Ihnen konkrete Suchbegriffe vor. Die obersten Treffer führen auf gefälschte Webseiten, die der apoBank-Webseite bzw. Login-Seite des apoBank-Online-Bankings zum Verwechseln ähnlich sehen, um dort Ihre Zugangsdaten oder andere persönliche Informationen abzufragen.

Geben Sie Internetadressen daher immer direkt in die Adresszeile Ihres Browsers ein und achten Sie darauf, dass es sich um eine Ihnen bekannte Adresse handelt. Lassen Sie sich nicht dazu überreden, abweichende Aufrufsvarianten zu nutzen.



Damit können unterschiedliche Straftaten (u. a. Betrug) begangen werden. Es lassen sich Online-Konten eröffnen, neue Zugangsdaten zum Online-Banking bestellen, Verträge abschließen oder Einkäufe auf Rechnung tätigen. Der tatsächliche Identitätsinhaber bemerkt den Missbrauch oft erst, wenn es bereits zu finanziellen Schäden oder rechtlichen Konsequenzen gekommen ist. Nachfolgend sind mögliche Szenarien dargestellt, die verdeutlichen, welche Auswirkungen ein Identitätsdiebstahl haben kann:

Mit Zugangsdaten (z. B. E-Mail-Adresse und Passwort) kann der Täter etwa:

- Zugriff auf Online-Konten (z. B. E-Mail, Amazon, PayPal, Social Media) erlangen.
- Bestellungen auf fremde Rechnung tätigen.
- Kommunikationsverläufe einsehen sowie manipulieren.

Persönliche Daten, wie Name, Geburtsdatum, Adresse und Bankdaten, ermöglichen etwa:

- das Eröffnen von Bankkonten oder Kreditkartenverträgen im Namen des Opfers.
- das Abschließen von Krediten oder Ratenverträgen.
- den Einkauf auf Rechnung in Online-Shops.

Wenn Social-Media-Konten übernommen werden, kann der Täter etwa:

- das Opfer öffentlich kompromittieren.
- Nachrichten an Freunde verschicken, um weitere Daten oder Geld zu erschleichen (z. B. durch „Ich bin in Not“-Nachrichten).
- Schadsoftware oder Phishing-Links verbreiten.

Langfristige Folgen für die Opfer

- **Finanzieller Schaden:** Verlust von Geld und Probleme mit der Schufa oder anderen Auskunfteien.
- **Rechtliche Probleme:** Mahnungen, Inkassoverfahren oder Strafanzeigen.
- **Psychischer Stress:** Gefühl des Kontrollverlusts, Unsicherheit und Vertrauensverlust hinsichtlich digitaler Dienste.
- **Aufwand zur Wiederherstellung der Identität:** Anzeige bei der Polizei, Sperrung von Konten, Identitätsnachweise erneuern etc.

Manipulation von sozialen Medien

Social-Media-Manipulation ist eine Methode, bei der Betrüger soziale Netzwerke nutzen, um gezielt Vertrauen aufzubauen und Informationen zu gewinnen. Dabei treten sie oft mit gefälschten Profilen auf und geben sich als bekannte Personen oder Kolleginnen und Kollegen aus.

Durch persönliche Nachrichten, gefälschte Freundschaftsanfragen oder gezielte Interaktionen schaffen sie Basisvertrauen, um später sensible Daten zu erfragen oder Phishing-Angriffe zu starten. Besonders effektiv ist diese Methode, weil sie auf zwischenmenschlicher Nähe, Hilfsbereitschaft und Vertrauen gründet.

Prüfen Sie bitte Freundschaftsanfragen von fremden Personen und lehnen Sie diese im Zweifelsfall ab.

**Identitätsdiebstahl:
Eine unterschätzte Gefahr**

Sobald der Täter an persönliche Daten gelangt – etwa durch gefälschte Anrufe, Phishing-Mails oder die zur Verfügung stehenden öffentlichen Personeninformationen, z. B. aus den sozialen Medien –, kann er sich als die betroffene Person ausgeben.

Empfehlungen für einen sicheren Umgang mit Online-Banking

Online-Banking bietet heute eine bequeme Möglichkeit dafür, Bankgeschäfte schnell und flexibel zu erledigen. Gleichzeitig nutzen Betrüger immer raffiniertere Methoden, um unbefugten Zugriff auf Konten zu erhalten und finanzielle Schäden zu verursachen. Mit einigen einfachen, aber wirkungsvollen Maßnahmen können Sie sich effektiv schützen:

1. Seien Sie aufmerksam und schützen Sie Ihre persönlichen Daten vor Betrügern

Teilen Sie Ihre persönlichen Daten, Zugangsdaten, TANs oder Bestätigungen von Aufträgen niemals telefonisch, schriftlich oder per E-Mail/SMS.

2. Verwenden Sie sichere Zugangsdaten

Wählen Sie ein starkes Passwort mit einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Ändern Sie Ihre Zugangsdaten regelmäßig und verwenden Sie für das Online-Banking der apoBank keine Passwörter, die Sie bereits anderswo nutzen.

3. Wählen Sie die Höhe Ihrer Kontolimits nach Bedarf

Wählen Sie die Höhe Ihrer Kontolimits mit Bedacht. Verändern Sie das Limit nach oben nur für bestimmte Transaktionen und passen es dann wieder auf den gewählten, für Sie passenden Standard an.

4. Achten Sie auf die Adresse der Website

Geben Sie Ihre Zugangsdaten nur auf der offiziellen Website der apoBank ein. Achten Sie darauf, dass die Adresse mit „https://“ beginnt und ein Schloss-Symbol im Browser angezeigt wird.

5. Öffnen Sie keine verdächtigen E-Mails oder Links

Seien Sie misstrauisch gegenüber E-Mails oder Nachrichten, die Sie dazu auffordern, Ihre Zugangsdaten zu bestätigen oder einen Link zum Online-Banking anzuklicken. Die apoBank fordert solche Daten oder Aktionen niemals per E-Mail an.

6. Halten Sie Ihre Systeme und Anwendungen stets auf dem aktuellen Stand

Regelmäßige Updates helfen dabei, Sicherheitslücken zu schließen und Schadsoftware abzuwehren.

7. Vermeiden Sie öffentliche WLANs

Nutzen Sie das Online-Banking der apoBank vorzugsweise in sicheren Netzwerken, da öffentliche WLANs ein erhöhtes Risiko für Datendiebstahl darstellen.

8. Regelmäßiger Login

Loggen Sie sich regelmäßig in Ihr apoBank-Online-Banking-Konto ein und kontrollieren Sie registrierte Geräte und Umsätze auf Korrektheit.

9. Beobachten Sie Ihre Kontobewegungen regelmäßig

Kontrollieren Sie Ihre Umsätze und Transaktionen regelmäßig, um ungewöhnliche Aktivitäten schnell zu erkennen und sofort zu reagieren.

10. Kontaktieren Sie die apoBank bei Unregelmäßigkeiten

Im Verdachtsfall sollten Sie umgehend die apoBank informieren und gegebenenfalls Online-Zugang und Karten sperren lassen.

11. Holen Sie sich bei ungewöhnlichen oder dringenden Anfragen stets eine Rückbestätigung ein

Kontaktieren Sie Mitarbeiter der apoBank direkt über bekannte und offizielle Kanäle, bevor Sie sensiblen Forderungen nachkommen.



Übrigens: Die Aktualisierung Ihrer persönlichen Daten, das Ändern von Passwörtern oder die Prüfung von Umsätzen etc. können Sie jederzeit über Ihr Kundenkonto durchführen – dazu ist kein gesondertes Formular/das Anklicken von Links in Mails etc. erforderlich. Auch technische Updates/Aktualisierungen des Online-Bankings erfordern nicht Ihre persönliche Mitwirkung.

Bei der Zusammenstellung dieser Informationen haben wir mit großer Sorgfalt gearbeitet. Dennoch können wir Fehler nicht ausschließen. Für die Richtigkeit und Vollständigkeit der Aussagen und Angaben übernehmen wir keine Haftung. Diese Information ersetzt keine individuelle Finanz-, Rechts- oder Steuerberatung. Stand: 12/2025.

Gefahr erkennen, Betrug vermeiden.

Notfall-Telefonnummern

Wenn Sie vermuten, Opfer eines Betrugs geworden zu sein, oder bereits Daten weitergegeben haben:

Kontaktieren Sie bitte umgehend unsere Betrugs-Hotline: **+49 211 59794 7777**
(Montag bis Freitag von 7 bis 20 Uhr,
Samstag von 9 bis 16 Uhr)

Debitkarte

Sperrannahme bei Verlust oder Diebstahl:
+49 116 116 (24-Stunden-Service)

Kreditkarten der apoBank

Sperrannahme bei Verlust oder Diebstahl,
Sperrannahmedienst bei VR Payment:
+49 721 120966001 (24-Stunden-Service)
oder **+49 116 116** (24-Stunden-Service)

Alternativ bei Verlust einer Kreditkarte oder Debitkarte der apoBank: Sofern Sie die **116 116** aus dem Ausland nicht erreichen: **+49 30 40 50 40 50** (telefonischer Vermittlungsdienst an die zuständige Sperrinstanz; bundesweit gebührenfrei) oder Sie melden sich bei Ihrer konto-führenden apoBank-Filiale (während der Geschäftszeiten).

Schützen Sie sich und Ihre Daten!

Konkrete Tipps finden Sie unter:

www.apobank.de/sicherheit

Herausgeber:

Deutsche Apotheker- und Ärztebank eG
Richard-Oskar-Mattern-Straße 6 | 40547 Düsseldorf

T 0211 5998 0
F 0211 5938 77
M info@apobank.de

apobank.de