



Banking mit dem Smartphone

Von der Bankfiliale bis zur Bank in der Hosentasche



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

So kennen wir Bankgeschäfte

Viele Jahre gehörten diese Dinge ganz selbstverständlich dazu.



Die Bankfiliale als Anlaufstelle
Beratung, Schalter, Öffnungszeiten



Überweisung auf Papier
Ausfüllen und in der Filiale abgeben



Sparbuch und Kontoauszüge
Drucker, Eintragungen, Papierbelege



Geld in bar
Bargeld abheben, einzahlen, zählen



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Was bedeutete „zur Bank gehen“?

Viele Bankgeschäfte waren nur in der Filiale möglich.



Geld abheben oder einzahlen

Am Schalter Bargeld erhalten oder einzahlen



Überweisung abgeben

Überweisungsträger ausfüllen und abgeben



Kontoauszüge und Belege

Ausdrucke am Schalter oder am Drucker holen



Dauerauftrag einrichten

Persönlich mit der Bank besprechen und einrichten



Beratung erhalten

Persönlicher Kontakt bei Fragen und Problemen



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Vom Papier zum Buchgeld

Vieles wurde einfacher – auch wenn wir es damals noch gar nicht „digital“ nannten.



Geld ist längst mehr als Bargeld

Ihr Gehalt, Ihre Rente, Miete, Strom – vieles läuft schon lange über Konten.



Überweisungen brauchen kein Papier mehr

Ihr Geld wird als Buchung von Konto zu Konto geschrieben – schnell und sicher.



Kontoauszüge und Belege

Statt Papier erhalten wir heute Auszüge und Belege als Ausdruck oder digital.



Alles im Blick

Wir können jederzeit sehen, was auf dem Konto los ist – ohne zur Bank gehen zu müssen.

Überweisung

Empfänger / Zahlungsempfänger

IBAN des Empfängers

Betrag: Euro, Cent

BIC

Kreditinstitut des Empfängers

Verwendungszweck

Kontoinhaber / Einzahler

IBAN Kontoinhaber

SPARBUCH

Datum	Eingang (Euro)	Ausgang (Euro)	Saldo (Euro)
02.01.	200,00		200,00
15.01.		- 50,00	150,00
31.01.	100,00		250,00
12.02.		- 30,00	220,00
28.02.	50,00		270,00
15.03.		- 70,00	200,00
31.03.	100,00		300,00
15.04.		- 40,00	260,00
			260,00
		Übertrag	



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Die Bank zog nach Hause

Mit dem Computer begann das Online-Banking.



Bankgeschäfte rund um die Uhr

Nicht mehr an Öffnungszeiten gebunden – von zu Hause und in Ruhe erledigen.



Überweisungen einfach online

Empfänger, Betrag und Verwendungszweck eingeben – sicher mit TAN bestätigen.



Konten und Umsätze im Blick

Kontostand prüfen, Umsätze anzeigen, Kontoauszüge herunterladen.



Daueraufträge und Vorlagen

Wiederkehrende Zahlungen einrichten und jederzeit anpassen.



Sicher und bequem

Verschlüsselte Verbindung, persönliche Zugangsdaten und TAN sorgen für Schutz.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Und schließlich: Die Bank in der Hosentasche

Mit dem Smartphone haben wir unsere Finanzen immer dabei.



Bankgeschäfte überall erledigen

Kontostand prüfen, Überweisen, Daueraufträge verwalten – jederzeit und fast überall.



Bezahlen mit dem Smartphone

Kontaktlos im Geschäft, online oder in Apps – schnell, einfach und hygienisch.



Sicherheit im Blick

Moderne Sicherheitsverfahren und TAN-Apps schützen unser Geld und unsere Daten.



Immer informiert

Umsätze in Echtzeit, Benachrichtigungen und wichtige Mitteilungen sofort erhalten.



Alles selbst in der Hand

Karten verwalten, Limits ändern, Dokumente abrufen – viele Dinge ohne Weg zur Bank erledigen.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Ist das eigentlich besser?

Neue Möglichkeiten bringen viele Vorteile – aber auch neue Herausforderungen.

Die Vorteile



24 Stunden verfügbar

Bankgeschäfte erledigen, wann es Ihnen passt – auch abends und am Wochenende.



Kein Weg zur Filiale

Zeit und Kosten sparen – alles bequem von zu Hause oder unterwegs.



Schnell und übersichtlich

Überweisungen in Sekunden, Kontostand sofort sehen, gute Übersicht.



Karte und Konto im Griff

Karte sperren, Limits ändern, alles direkt in der App erledigen.



Weniger Papier, gut für die Umwelt

Kontoauszüge digital statt Papierberge – übersichtlich und dauerhaft gespeichert.

Die Nachteile



Weniger persönlicher Kontakt

Beratung und Hilfe vor Ort werden immer seltener.



Abhängigkeit von Technik

Smartphone, Internet und Akku sind notwendig – nicht immer sicher.



Neue Betrugsformen

Phishing, falsche Anrufe, gefälschte Mails – Vorsicht ist wichtiger denn je.



Überforderung möglich

Neue Apps und Verfahren können verunsichern und stressen.



Nicht für alle geeignet

Menschen ohne Smartphone oder Interesse dürfen nicht abgehängt werden.



Es geht nicht darum, alles nur noch digital zu machen – sondern die Wahl zu haben!



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Bargeld, Karte und Smartphone sind Werkzeuge.

Sie entscheiden, welches Werkzeug Sie benutzen möchten.



Bargeld Stark im Alltag



Funktioniert immer

Ohne Akku, ohne Smartphone, ohne Internet.



Privatsphäre

Zahlungen bleiben anonym – keine Daten werden gespeichert.



Bessere Ausgabenkontrolle

Man sieht und spürt, was man ausgibt.



Überall einsetzbar

Auch dort, wo Karten oder Apps nicht funktionieren.



Digitales Bezahlen Stark in vielen Situationen



Bequem und schnell

Zahlungen in Sekunden erledigt – überall und rund um die Uhr.



Nachvollziehbar

Umsätze im Blick, Kategorien, Auswertungen und Erinnerungen.



Neue Möglichkeiten

Online-Shopping, Tickets, Abos, Daueraufträge und vieles mehr.



Kontaktlos bezahlen

Mit Karte oder Smartphone – einfach, hygienisch und sicher.



Beide Formen haben ihren Platz – je nach Situation, Bedarf und persönlicher Präferenz.
Wichtig ist, dass Sie die Wahl haben und wissen, wie es funktioniert.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Mobiles Bezahlen – einfach, schnell und sicher

Mit Smartphone oder Smartwatch an der Kasse bezahlen – statt Bargeld oder Karte.

Kontaktlos. Bequem. Sicher.



Wichtig: Funktioniert nur dort, wo das **Kontaktlos-Symbol**  am Terminal oder an der Kasse zu sehen ist.

Wie funktioniert mobiles Bezahlen?

Sie bezahlen mit Apple Pay oder Google Pay, indem Sie Ihr Smartphone oder Ihre Smartwatch an das Terminal halten.

-  **Karte hinterlegen**
Ihre Bankkarte wird einmalig in Apple Wallet oder Google Wallet hinterlegt.
-  **Gerät entsperren**
Entsperren Sie Ihr Smartphone oder Ihre Smartwatch mit Face ID, Touch ID, Fingerabdruck oder PIN.
-  **An das Terminal halten**
Halten Sie Ihr Gerät einige Zentimeter an das Kontaktlos-Symbol am Terminal.
-  **Bezahlung ist erledigt**
Ein Signal oder eine Meldung bestätigt die Zahlung – fertig!

 **Tipp:** Kleine Beträge bis 25 € funktionieren oft ohne Entsperren, größere Beträge fast immer mit Entsperren.

Wie sicher ist mobiles Bezahlen?

Sehr sicher – oft sicherer als Karte oder Bargeld. Denn Ihre echten Kartendaten werden nicht weitergegeben.

-  **Keine Kartendaten beim Bezahlen**
Beim Bezahlen wird keine echte Kartennummer übertragen, sondern eine einmalige Gerätenummer (Token).
-  **Nur Sie können bezahlen**
Ihr Gerät muss entsperrt sein oder Sie bestätigen sich mit Fingerabdruck, Gesicht oder PIN.
-  **Verlustschutz**
Bei Verlust können Sie Ihr Gerät aus der Ferne sperren und Ihre Karten sofort in der App deaktivieren.
-  **Jede Zahlung ist einzigartig**
Für jede Zahlung wird ein neuer Code (Token) erzeugt – ein Diebstahl der Daten bringt nichts.
-  **Sicher durch moderne Technik**
Apple Pay und Google Pay nutzen modernste Sicherheitstechnologien und werden laufend geprüft.

 **Tipp:** Nutzen Sie immer eine Geräte-Sperre (PIN, Fingerabdruck, Gesichtserkennung) – das erhöht Ihre Sicherheit zusätzlich.

Ihre Vorteile

-  **Schnell**
Smartphone entsperren, ans Terminal halten, fertig – in wenigen Sekunden bezahlt.
-  **Bequem**
Kein Bargeld suchen, keine Karte einstecken – alles in Ihrem Gerät.
-  **Überall nutzbar**
Weltweit dort bezahlen, wo kontaktloses Bezahlen akzeptiert wird.
-  **Weniger ist mehr**
Sie brauchen nur Ihr Smartphone oder Ihre Smartwatch – nicht Ihre ganze Geldbörse.
-  **Übersicht in der App**
Alle Zahlungen sehen Sie sofort in Ihrer Banking-App.

 **Gut zu wissen:**
In Geschäften können Sie wie gewohnt Punkte sammeln und auch Kundenkarten in der App nutzen (z. B. Payback).

Vergleich: Bargeld, Karte oder mobil?

	 Bargeld	 Karte	 Mobil
Schnell	–	○	✓
Bequem	–	○	✓
Kontaktlos	○	✓	✓
Hygienisch	○	✓	✓
Sicher	○	✓	✓✓
Weltweit nutzbar	–	○	✓
Kein Kleingeld	✓	✓	✓



Unser Fazit:
Mobiles Bezahlen verbindet die Vorteile von Karte und Bargeld – und macht das Bezahlen noch einfacher und sicherer.



Wichtig zu beachten
Nicht jedes Geschäft akzeptiert mobiles Bezahlen. Achten Sie auf das Kontaktlos-Symbol am Terminal.



Für mobile Zahlungen benötigen Sie einen geladenen Akku.



Eine Internetverbindung ist für die Zahlung meist nicht nötig – nach dem Einrichten funktioniert es auch offline.



Bei Gerätverlust: Sofort aus der Ferne sperren und Karten in der App deaktivieren.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Was kostet digitales Bezahlen wirklich?

Bei jeder digitalen Zahlung erhält ein Dienstleister einen Anteil.

Diese Kosten zahlen letztlich Sie – oft indirekt.



Zahlungsart	Wer ist beteiligt?	Typische Kosten*	Wer trägt die Kosten?
PayPal	Kunde – PayPal – Händler/Empfänger	ca. 1,9 % – 2,9 % + 0,35 € pro Zahlung	Händler/Empfänger (meist im Preis berücksichtigt)
Klarna (Rechnung)	Kunde – Klarna – Händler	ca. 1,9 % – 3,5 % + ggf. feste Gebühr	Händler (teilweise auf Produkte umgelegt)
Kreditkarte (Visa/Mastercard)	Kunde – Bank – Karten- netzwerk – Händler	ca. 0,5 % – 1,5 % + ggf. feste Gebühr	Händler (meist im Preis berücksichtigt)
Apple Pay / Google Pay	Kunde – Bank – Karten- netzwerk – Händler	ähnlich wie Kreditkarte (0,5 % – 1,5 %)	Händler (meist im Preis berücksichtigt)
Überweisung (Echtzeit)	Kunde – Bank des Kunden – Bank des Empfängers	häufig kostenlos, manchmal 0,20 € – 0,50 €	Kunde (bei der eigenen Bank)
Echtzeit- Überweisung	Kunde – Bank – Bank des Empfängers	häufig kostenlos, manchmal 0,20 € – 0,50 €	Kunde (bei der eigenen Bank)

* Richtwerte (Stand 2024/25). Je nach Anbieter, Vertrag und Umfang können die Kosten abweichen.

Was bedeutet das für Sie?



Händler geben die Kosten meist an alle Kunden weiter – auch an Sie.



Je teurer die Zahlungsart für den Händler, desto höher können Preise sein.



Bei kleinen Beträgen oder häufigen Zahlungen summiert sich der Anteil schnell.



Manche Anbieter sind kostenlos – aber nicht alle Serviceleistungen.



Es lohnt sich, die passende Zahlungsart zu wählen.

Beispiel:



Einkauf im Supermarkt
Warenwert: 50,00 €



Barzahlung
Kosten für den Händler:
0,00 €



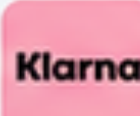
Kartenzahlung
(EC-/Debitkarte)
Kosten für Händler:
ca. 0,20 € – 0,50 €



Kreditkarte
Kosten für Händler:
ca. 0,60 € – 1,00 €



PayPal
Kosten für Händler:
ca. 1,00 € – 1,50 €



Klarna (Rechnung)
Kosten für Händler:
ca. 1,00 € – 1,75 €

Diese Beträge wirken klein – aber bei vielen Transaktionen und kleinen Margen machen sie einen großen Unterschied.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Was kann meine Banking-App?

Ihre Banking-App bringt die wichtigsten Bankgeschäfte auf Ihr Smartphone – sicher, bequem und rund um die Uhr.

Die Funktionen können je nach Bank etwas variieren.



Kontostände & Umsätze

Aktuellen Kontostand einsehen und alle Buchungen im Blick behalten.



Überweisungen

Einzelüberweisungen und Daueraufträge erstellen und verwalten.



Echtzeit-Überweisung

Geld in wenigen Sekunden ankommt – auch außerhalb der Geschäftszeiten.



Daueraufträge & Vorlagen

Regelmäßige Zahlungen einrichten, ändern oder pausieren.



Dokumente & Postfach

Kontoauszüge, Steuerbescheinigungen und Bankpost digital abrufen.



Kartenverwaltung

Karten sperren, entsperren, Limits ändern und Kartendetails einsehen.



Mobiles Bezahlen

Mit dem Smartphone bezahlen – im Geschäft und online (z. B. mit Apple Pay / Google Pay).



Empfängerverwaltung

Empfänger speichern, bearbeiten und schnell auswählen.



Finanzübersicht & Auswertung

Einnahmen und Ausgaben kategorisieren und grafisch auswerten.



Benachrichtigungen

Umsätze, Gehaltseingang oder Kartenzahlungen in Echtzeit informiert bekommen.



Sicherheit & Einstellungen

Zugänge verwalten, Geräte autorisieren und Sicherheitseinstellungen anpassen.



Tipp: Schauen Sie sich in Ihrer App in Ruhe um. Viele Funktionen entdecken Sie erst, wenn Sie ein wenig Zeit zum Ausprobieren nehmen.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**

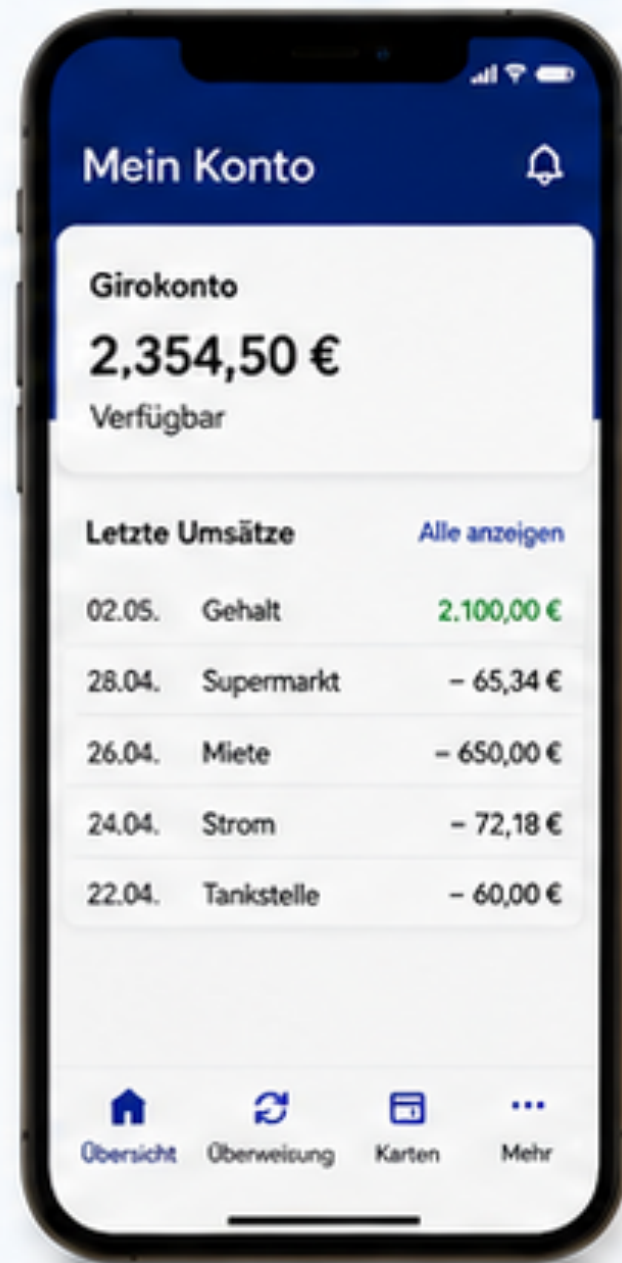


Referent:
Martin Adam

Banking-App und TAN-App – warum zwei Apps?

Viele Banken nutzen zwei verschiedene Apps.
Das hat einen guten Grund: **Ihre Sicherheit.**

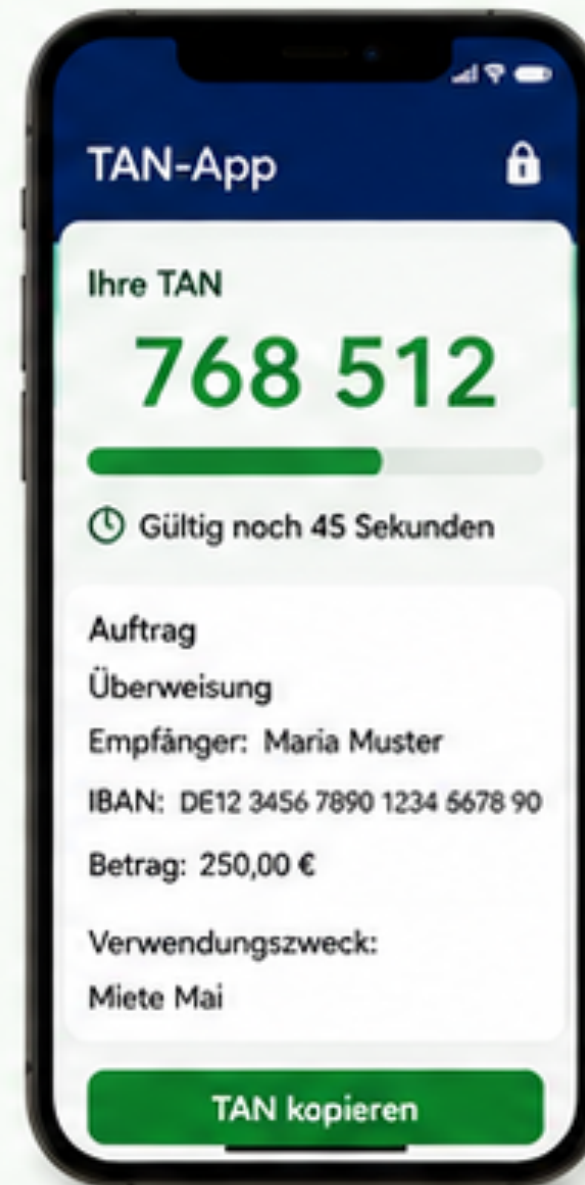
1. Die Banking-App



Mit der Banking-App erledigen Sie Ihre Bankgeschäfte:

- Kontostand & Umsätze** einsehen
- Überweisungen** erstellen
- Daueraufträge** verwalten
- Karten & Limits** verwalten
- Dokumente** abrufen
- Nachrichten** empfangen

2. Die TAN-App



Die TAN-App erzeugt **Einmal-Codes** für Ihre Aufträge.

- Jede TAN ist nur für einen bestimmten Auftrag gültig.
- Die TAN ist nur kurze Zeit gültig (z. B. 60 Sekunden).
- Ohne TAN kann niemand einen Auftrag bestätigen.

Die TAN-App enthält **keine** Kontodaten und kann **keine** Überweisungen ausführen.

Warum zwei Apps mehr Sicherheit bieten

- Schutz bei Schadsoftware**
Würde Schadsoftware auf Ihrem Smartphone die Banking-App manipulieren, könnte sie keine TAN erzeugen.
- Getrennte Funktionen**
Bankgeschäfte und TAN-Erzeugung sind technisch getrennt.
- Zusätzliche Kontrolle**
Sie prüfen in der TAN-App die Details des Auftrags, bevor Sie die TAN eingeben.
- Empfehlung der Banken**
Das Zwei-App-Verfahren ist ein anerkannter Sicherheitsstandard.



Tipp: Installieren Sie beide Apps nur von der offiziellen Website Ihrer Bank oder aus dem App Store / Google Play Store.
Geben Sie Ihre TAN **niemals** weiter – auch nicht an angebliche Mitarbeiter Ihrer Bank.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Ist Smartphone-Banking sicher?

Ja – wenn Sie selbst ein paar wichtige Regeln beachten.

Ihre Bank nutzt moderne Sicherheitsverfahren,
aber auch Sie spielen eine wichtige Rolle.

Darauf können Sie sich verlassen



Banken nutzen starke Sicherheit

Verschlüsselte Verbindungen, gesicherte Apps und moderne Verfahren schützen Ihre Daten.



Zwei-Faktor-Authentifizierung (2FA)

Wichtige Aufträge müssen Sie zusätzlich bestätigen – z. B. mit TAN oder Biometrie.



Geräteschutz

Zugriff auf Ihre App ist durch PIN, Fingerabdruck oder Gesichtserkennung geschützt.



Überwachung rund um die Uhr

Auffällige Aktivitäten werden erkannt und gestoppt.



Sie haben die Kontrolle

Sie können Geräte verwalten, Zugänge prüfen und Karten sofort sperren.



Moderne
Sicherheits-
verfahren
schützen Ihr
Konto.

Bleibende Risiken – deshalb vorsichtig sein



Betrüger werden immer raffinierter

Phishing, falsche Anrufe, gefälschte Nachrichten – sie wollen an Ihre Daten und TANs.



Öffentliche WLANs sind unsicher

Nutzen Sie für Banking besser Ihr Mobilfunknetz oder ein sicheres WLAN zu Hause.



Verlust oder Diebstahl des Smartphones

Sperren Sie Ihr Gerät (PIN/biometrisch) und richten Sie „Mein Gerät finden“ ein.



Apps nur aus offiziellen Quellen

Installieren Sie Apps nur aus App Store oder Google Play – keine unbekannten Quellen.



Sie machen den Unterschied

Geben Sie niemandem Ihre Zugangsdaten oder TANs – auch nicht auf Aufforderung.



Tipp: Aktualisieren Sie regelmäßig Ihr Smartphone und Ihre Banking-App.
So schließen Sie Sicherheitslücken und bleiben auf dem neuesten Stand.



Merksatz: Technik schützt –
Aufmerksamkeit noch mehr.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Zeitdruck ist ein Warnsignal

Betrüger setzen Sie unter Druck, damit Sie nicht mehr nachdenken oder mit anderen sprechen können.

Nehmen Sie sich Zeit – es geht um Ihr Geld und Ihre Sicherheit!

Typische Aussagen der Betrüger

-  „Wenn Sie jetzt nicht handeln, wird Ihr Konto gesperrt.“
-  „Ihre Karte wird missbraucht – bestätigen Sie das bitte sofort!“
-  „Das Angebot gilt nur heute – sonst verlieren Sie Ihr Geld.“
-  „Ihr Paket kann nur jetzt zugestellt werden – bezahlen Sie schnell.“
-  „Das ist eine sichere Verbindung – geben Sie jetzt Ihre TAN ein.“



Tipp: Überweisen, TAN eingeben oder Daten weitergeben können Sie auch später noch. Betrüger verschwinden, sobald Sie Zeit gewinnen.



So schützen Sie sich

-  **Nehmen Sie sich Zeit.**
Echte Banken drängen Sie niemals.
-  **Pause machen.**
Atmen Sie tief durch und überlegen Sie in Ruhe.
-  **Rückruf statt Rückrufnummer.**
Legen Sie auf und rufen Sie Ihre Bank selbst an – über die Nummer auf Ihrer Karte oder der Website.
-  **Mit jemandem sprechen.**
Fragen Sie eine Vertrauensperson um Rat.

Merken Sie sich diese 4 Fragen



Warum der Zeitdruck?

Wer ehrlich ist, hat Zeit für Ihre Fragen.



Was passiert wirklich?

Bleibt Ihr Konto wirklich nicht mehr verfügbar? Prüfen Sie es in Ruhe.



Wer ist mein Ansprechpartner?

Nutzen Sie nur die offiziellen Kontakte Ihrer Bank.



Bin ich mir sicher?

Im Zweifel: Stopp! Lieber einmal zu viel nachfragen als Geld verlieren.



Unser wichtigster Rat:

Zeitdruck ist kein Zufall – er ist Teil des Betrugs.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Ihre Bank ruft an – oder doch nicht?

Betrüger geben sich am Telefon als Bankmitarbeiter aus, um an Ihre Daten oder Ihr Geld zu kommen.

Misstrauen Sie – schützen Sie sich!

Typische Merkmale betrügerischer Anrufe



Unerwarteter Anruf

Sie werden angerufen, obwohl Sie Ihre Bank nicht kontaktiert haben.



Zeitdruck

Der Anrufer drängt Sie zu schnellen Entscheidungen.



Aufforderung zu sensiblen Daten

Es werden PIN, TAN, Passwörter oder die Kartennummer verlangt.



Fernzugriff gefordert

Sie sollen eine App installieren oder den Bildschirm freigeben.



Ungewöhnliche Bitte

Sie sollen Geld überweisen oder Ihre Karte an einen Boten übergeben.



Tipp: Speichern Sie die offizielle Telefonnummer Ihrer Bank im Smartphone – so haben Sie sie im Zweifel immer griffbereit.



So verhalten Sie sich richtig



Gespräch beenden.

Legen Sie einfach auf, wenn Sie unsicher sind.



Selbst anrufen.

Rufen Sie Ihre Bank nur über die offizielle Telefonnummer an – nicht über die Nummer, die der Anrufer nennt.



Keine Daten preisgeben.

Ihre Bank fragt niemals nach PIN, TAN oder Passwörtern.



Nichts installieren oder freigeben.

Erlauben Sie keinen Fernzugriff auf Ihr Smartphone oder Ihren Computer.



Mit jemandem sprechen.

Fragen Sie eine Vertrauensperson um Rat.

Merken Sie sich diese 5 Regeln



Misstrauisch sein.

Unerwarteter Anruf? Erst denken, dann handeln.



Offizielle Nummer nutzen.

Kontakte Ihrer Bank finden Sie auf Ihrer Bankkarte, im Kontoauszug oder auf der Website Ihrer Bank.



Keine sensiblen Daten am Telefon.

PIN, TAN, Passwörter und Kartendaten bleiben privat.



Nichts installieren oder freigeben.

Ihre Bank braucht keinen Zugriff auf Ihr Gerät.



Im Zweifel nachfragen.

Lieber einmal zu viel prüfen als Geld verlieren.



Wichtig zu wissen:

Ihre Bank wird Sie niemals auffordern, Geld zu überweisen oder Ihre Karte oder PIN herauszugeben.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Die SMS von der Bank

Betrüger verschicken gefälschte SMS, um an Ihre Daten oder Ihr Geld zu gelangen.

Erkennen Sie die Tricks – handeln Sie richtig!

Typische Merkmale gefälschter SMS

-  **Dringlichkeit und Angst**
Die SMS erzeugt Zeitdruck und verunsichert Sie.
-  **Links zu gefälschten Webseiten**
Im Link werden Sie aufgefordert, Ihre Daten einzugeben.
-  **Unpersönliche Anrede**
Es gibt keine persönliche Ansprache, sondern nur „Sehr geehrter Kunde“.
-  **Rechtschreib- und Grammatikfehler**
Hinweis auf unseriöse Absender.
-  **Aufforderung zur Kontaktaufnahme**
Sie sollen eine Nummer anrufen oder auf den Link klicken.



Unpersönlich

Ihre Bank kennt Ihren Namen.

Zeitdruck

„sofort“ und „Sperrung“ sollen Sie unter Druck setzen.

Verdächtiger Link

Der Link sieht ähnlich aus, führt aber nicht zur Website Ihrer Bank.

Allgemeiner Absender

Keine bekannte Nummer Ihrer Bank.



Ihre Bank wird Sie niemals per SMS auffordern, Ihre Daten zu bestätigen oder einen Link zu klicken!

5 goldene Regeln



Bleiben Sie ruhig.

Nehmen Sie sich Zeit und lassen Sie sich nicht unter Druck setzen.



Klicken Sie keine Links an.

Öffnen Sie keine Links in SMS oder E-Mails von unbekannten Absendern.



Kontaktieren Sie Ihre Bank selbst.

Rufen Sie die offizielle Nummer Ihrer Bank an oder nutzen Sie Ihre Banking-App.



Geben Sie keine Daten preis.

Teilen Sie niemandem PIN, TAN, Passwörter oder Kartendaten mit.



Sprechen Sie mit jemandem.

Im Zweifel fragen Sie eine Vertrauensperson um Rat.



Im Zweifel: Nicht reagieren!

Löschen Sie die SMS und melden Sie den Vorfall bei Ihrer Bank.



Tipp: Prüfen Sie regelmäßig in Ihrer Banking-App, ob alle Mitteilungen echt sind. Aktivieren Sie Benachrichtigungen in der App statt per SMS – das ist sicherer.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Phishing per Mail, WhatsApp & Co.

Betrüger versuchen, Sie mit gefälschten Nachrichten zu täuschen, um an Ihre Daten oder Ihr Geld zu kommen.

Erkennen Sie die Tricks – schützen Sie sich!

Typische Phishing-Tricks



Vortäuschung von Absendern

Die Nachricht sieht aus, als käme sie von Ihrer Bank, einem Paketdienst oder einer Behörde.



Dringlichkeit und Angst

Sie werden aufgefordert, schnell zu handeln – sonst drohen Sperrung, Kosten oder Verlust.



Lockangebote

Gewinne, Gutscheine oder tolle Angebote sollen Sie zum Klicken verleiten.



Aufforderung zur Dateneingabe

Sie sollen PIN, TAN, Passwörter oder Kreditkartendaten eingeben.



Anhänge mit Schadsoftware

Dateien oder Links können Viren oder Schadprogramme enthalten.



Tipp: Ihre Bank kommuniziert wichtige Informationen in der Banking-App, per Brief oder über sichere Nachrichten. Aktivieren Sie Benachrichtigungen in der App – so erhalten Sie echte Mitteilungen direkt und sicher.

Beispiele gefälschter Nachrichten



E-Mail

Gefälschte E-Mail von Ihrer Bank

Wichtige Sicherheitsinformation von Ihrer Bank

Von: service@ihre-bank-secure.com
An: Sie

Sehr geehrte Kundin, sehr geehrter Kunde,

wir haben ungewöhnliche Aktivitäten auf Ihrem Konto festgestellt. Bitte überprüfen Sie Ihre Daten, um eine Sperrung zu vermeiden.

[> Jetzt anmelden](#)

Mit freundlichen Grüßen
Ihre Bank



Verdächtig:

Absender, Rechtschreibung, Link und Aufforderung.



WhatsApp

Nachricht von einem „Bekannten“

< +49 173 1234567 online

Hallo! Ich habe ein neues Handy und meine Nummer hat sich geändert. Kannst du mir kurz einen Gefallen tun? 11:42

Klar, was ist denn? 11:42 ✓

Super! Ich muss schnell eine Rechnung bezahlen. Kannst du mir 200 € per Überweisung schicken? IBAN: DE12 3456 7890 1234 5678 90
Danke dir! 11:44



Verdächtig:

Neue Nummer, Geldforderung, Druck und IBAN.



SMS

Gefälschte SMS („Smishing“)

IhreBank
Heute, 10:15

Ihre Bank:
Aus Sicherheitsgründen wurde Ihr Zugang eingeschränkt. Bitte bestätigen Sie Ihre Daten sofort, um die Sperrung zu vermeiden.

<https://ihre-bank-login.com>



Verdächtig:

Druck, Link und unbekannte Adresse.

So schützen Sie sich



Nachricht genau prüfen

Achten Sie auf Absender, Sprache, Rechtschreibung und ungewöhnliche Aufforderungen.



Keine Links anklicken

Öffnen Sie keine Links in E-Mails, SMS oder Chats – auch nicht in WhatsApp.



Keine Daten preisgeben

Ihre Bank fragt niemals nach PIN, TAN, Passwörtern oder Kartendaten.



Über offiziellen Weg prüfen

Im Zweifel: Kontaktieren Sie Ihre Bank über die offizielle Rufnummer oder die Banking-App.



Löschen & melden

Verdächtige Nachrichten löschen und bei Ihrer Bank oder Polizei melden.



Wichtig:

Im Zweifel lieber einmal zu viel prüfen als einmal zu wenig!



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

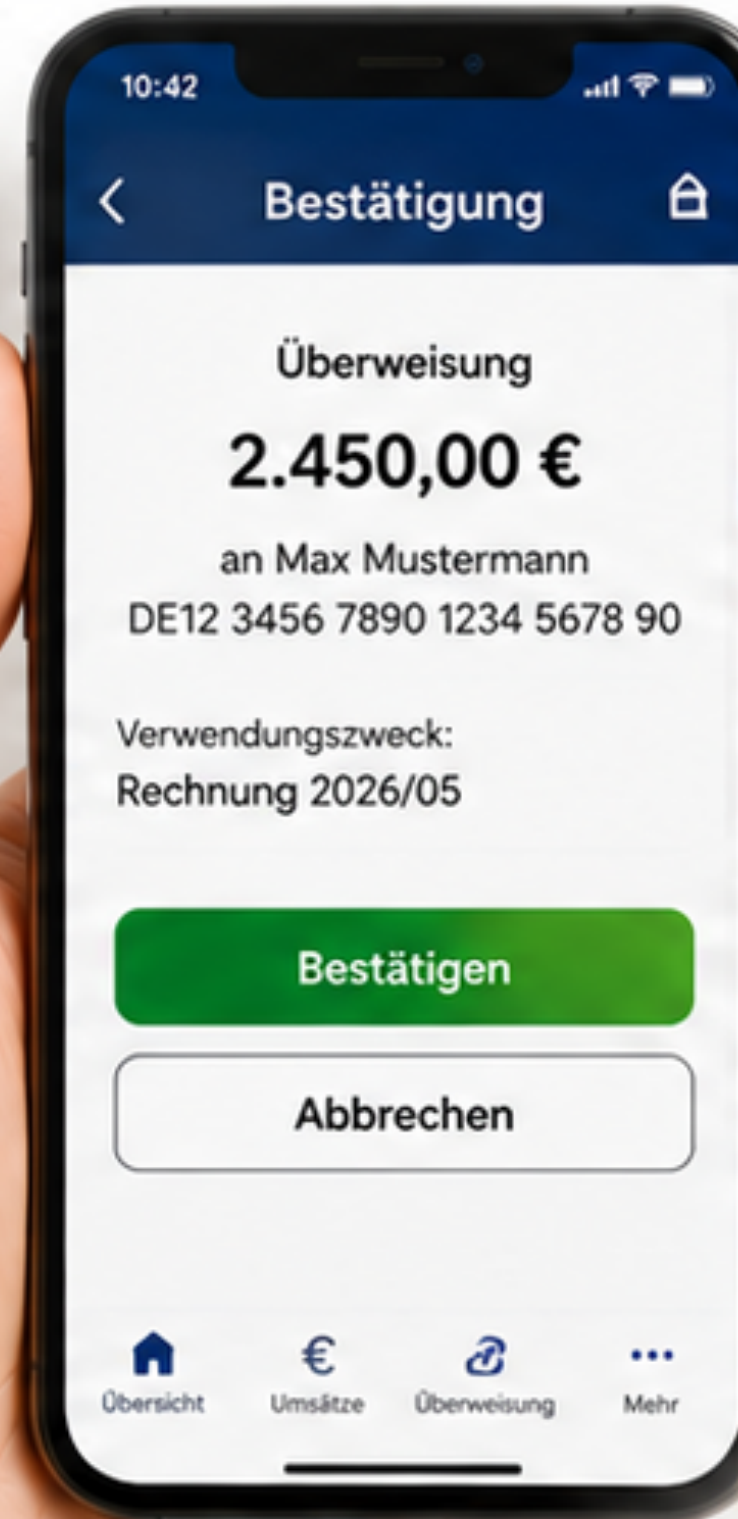
„Bestätigen Sie das bitte kurz in Ihrer App“

Betrüger geben sich als Bankmitarbeiter aus und bringen Sie dazu, selbst eine Bestätigung in Ihrer App zu machen.

Erkennen Sie die Masche – schützen Sie sich!

So läuft der Betrug ab

-  **1 Sie werden angerufen.**
Der Anrufer behauptet, Mitarbeiter Ihrer Bank zu sein.
-  **2 Es gibt ein „Problem“.**
Z. B. verdächtige Buchung, neues Gerät oder Datenleck.
-  **3 Sie sollen „kurz bestätigen“.**
Der Anrufer bittet Sie, eine Bestätigung in Ihrer Banking-App zu bestätigen.
-  **4 Ihr Geld ist in Gefahr.**
Mit Ihrer Bestätigung gibt der Betrüger Überweisungen frei oder richtet ein neues Gerät ein.



„Bitte bestätigen Sie das jetzt kurz in Ihrer App, damit wir Ihr Konto schützen können.“



Wichtig zu wissen:

-  Ihre Bank wird Sie **niemals** anrufen und um eine Bestätigung in der App bitten.
-  **Echte Bankmitarbeiter** haben bereits alle nötigen Rechte – sie brauchen keine Bestätigung von Ihnen.
-  Im Zweifel: Legen Sie auf und rufen Sie Ihre Bank über **die offizielle** Rufnummer selbst an.

5 Regeln für Ihre Sicherheit

-  **Nicht unter Druck setzen lassen.**
Betrüger wollen, dass Sie schnell und ohne Nachdenken handeln.
-  **Keine Bestätigungen auf Aufforderung.**
Bestätigen Sie in der App nur, wenn Sie selbst eine Überweisung oder Änderung beauftragt haben.
-  **Gespräch beenden.**
Legen Sie auf, wenn Sie unsicher sind.
-  **Bank selbst anrufen.**
Nutzen Sie nur die offizielle Rufnummer Ihrer Bank – nicht die Nummer, die Ihnen genannt wurde.
-  **Mit jemandem sprechen.**
Fragen Sie eine Vertrauensperson um Rat.

-  **Merken Sie sich:**
Ihre Bank benötigt nie Ihre Hilfe in der App – sie schützt Ihr Konto, nicht Sie das Konto der Bank!



Tipp: Aktivieren Sie Benachrichtigungen in Ihrer Banking-App.
So erkennen Sie sofort, wenn etwas in Ihrem Konto passiert.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Smartphone oder Karte verloren

Schnelles Handeln schützt Ihr Geld und Ihre Daten.

Sperren Sie sofort – je schneller Sie reagieren, desto besser!

Was kann passieren?



Missbrauch Ihrer Banking-App

Unbefugte können Zahlungen auslösen oder Kontodaten einsehen.



Missbrauch Ihrer Bankkarte

Mit Ihrer Karte können Einkäufe getätigt und Geld abgehoben werden.



Zugriff auf persönliche Daten

E-Mails, Nachrichten und Passwörter können ausgelesen werden.



Änderung von Zugangsdaten

Betrüger könnten Passwörter ändern und Sie aussperren.



Finanzielle Schäden

Je länger Unbekannte Zugriff haben, desto größer der Schaden.



Sofortmaßnahmen – in dieser Reihenfolge

- 1 Gerät sichern**
Falls möglich: Bildschirm sperren (PIN, Muster, Gesicht).
- 2 Banking-App sperren**
Über die App einer anderen Person oder im Online-Banking.
- 3 Bankkarte sperren**
Über die Banking-App, Online-Banking oder telefonisch.
- 4 SIM-Karte sperren**
Rufen Sie Ihren Mobilfunkanbieter an.
- 5 Verlust melden**
Erstatten Sie Anzeige bei der Polizei (bei Diebstahl).



5 Tipps für den Ernstfall



Sperr-Notruf 116 116

Rund um die Uhr erreichbar – kostenfrei aus dem deutschen Festnetz und Mobilfunk.



Wichtige Kontakte speichern

Speichern Sie Bank, Mobilfunkanbieter und Sperr-Notruf im Telefon und schriftlich.



Starke Bildschirmsperre nutzen

PIN, Muster oder biometrische Sperre schützt vor unbefugtem Zugriff.



Ortungsfunktion aktivieren

Erhöht die Chance, Ihr Gerät wiederzufinden oder zu sichern.



Regelmäßig sichern

So bleiben Ihre Daten erhalten, auch wenn das Gerät weg ist.



Wichtig!

Handeln Sie sofort – jede Minute zählt! Zögern kann teuer werden.



Tipp: Aktivieren Sie „Mein Gerät finden“ (Android) oder „Wo ist?“ (iPhone) und testen Sie die Funktion vorher. Bewahren Sie wichtige Rufnummern (z. B. Bank, Sperr-Notruf 116 116) griffbereit auf.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Ich bin darauf hereingefallen – was jetzt?

Das kann jedem passieren. Wichtig ist, jetzt schnell und richtig zu handeln.

Ruhe bewahren – handeln – Schaden begrenzen!

Woran erkennen Sie, dass etwas schiefgelaufen sein könnte?



Seltsame Nachrichten

E-Mail, SMS oder Anruf war dringlich oder ungewöhnlich.



Sie haben geklickt

Sie haben auf einen Link geklickt oder eine Datei geöffnet.



Daten eingegeben

Sie haben PIN, TAN, Passwörter oder Kartendaten eingegeben.



In einer fremden App bestätigt

Sie haben eine Überweisung oder Änderung in einer App bestätigt, die Sie jetzt als verdächtig erkennen.



Geld verschwunden oder unbekannt

Geld ist weg oder es wurden unbekannte Buchungen durchgeführt.



Tipp: Schreiben Sie sich wichtige Rufnummern auf und bewahren Sie sie getrennt auf. So sind Sie im Ernstfall schnell handlungsfähig.

Sofortmaßnahmen – keine Minute verlieren!

1

Verbindung trennen

Schließen Sie die Webseite/den Chat und klicken Sie nicht weiter. Trennen Sie gegebenenfalls WLAN.



2

Banking-App sperren

Sperren Sie Ihre Banking-App sofort in der App oder im Online-Banking.



3

Karten sperren

Sperren Sie Ihre Bankkarte(n) in der App oder rufen Sie Ihre Bank an.



4

Passwörter ändern

Ändern Sie Passwörter, die Sie eingegeben haben – besonders E-Mail, Online-Banking und wichtige Konten.



5

Bank kontaktieren

Rufen Sie sofort Ihre Bank an und schildern Sie den Vorfall. Fragen Sie nach, ob bereits Buchungen erfolgt sind.



6

Anzeige erstatten

Erstatten Sie Anzeige bei der Polizei – online oder vor Ort. Das ist wichtig für die weitere Bearbeitung.



Wichtig: Sie sind nicht schuld!

Betrüger sind sehr geschickt. Entscheidend ist, wie Sie jetzt reagieren. Je schneller Sie handeln, desto größer die Chance, den Schaden zu begrenzen.

So vermeiden Sie größeren Schaden



Keine weiteren Aktionen

Klicken, bestätigen oder zahlen Sie nichts weiter. Stoppen Sie jeden Kontakt.



Konten und Apps überprüfen

Prüfen Sie alle Konten und Apps auf ungewöhnliche Aktivitäten.



Buchungen kontrollieren

Überprüfen Sie Ihre Umsätze und informieren Sie Ihre Bank über verdächtige Buchungen.



Beweise sichern

Speichern Sie Nachrichten, E-Mails, Screenshots und Rufnummern als Beweis.



Mit jemandem sprechen

Besprechen Sie den Vorfall mit einer Vertrauensperson. Gemeinsam sieht man klarer.



Wichtige Kontakte

- Ihre Bank: Hotline auf der Rückseite Ihrer Karte oder auf der Website
- Sperr-Notruf 116 116 (rund um die Uhr)
- Polizei: 110



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Überweisungen – sicher und richtig

Eine Überweisung ist schnell gemacht – und Geld ist oft in Sekunden weg.

Prüfen Sie immer genau – bevor Sie bestätigen!

Typische Betrugsmaschen



Falsche Rechnung

Sie erhalten eine gefälschte Rechnung mit neuer Bankverbindung.



CEO-Fraud

Betrüger geben sich als Vorgesetzte oder Firmenleitung aus und fordern eine dringende Überweisung.



Schockanrufe / Notfälle

Sie werden unter Druck gesetzt und sollen sofort Geld für einen angeblichen Notfall überweisen.



Kauf im Internet

Bezahlung für Ware oder Dienstleistung – aber die Ware wird nie geliefert.



Gefälschte Zahlungsaufforderungen

E-Mails oder Nachrichten sehen echt aus – sind aber gefälscht.

Vor jeder Überweisung prüfen!



Empfänger prüfen

Ist der Name und die IBAN korrekt?
Passt der Empfänger zur Rechnung?



Rechnung prüfen

Ist die Rechnung wirklich von dem Absender?
Achten Sie auf ungewöhnliche Aufforderungen oder Änderungen.



Betrag prüfen

Ist der Betrag plausibel und korrekt?



Verwendungszweck prüfen

Achten Sie auf Rechtschreibfehler oder ungewöhnliche Formulierungen.



Keine Hektik

Niemals unter Zeitdruck handeln.
Im Zweifel: nachfragen!



Tipp: Speichern Sie häufige Empfänger als Vorlage.
So vermeiden Sie Tippfehler bei IBAN und Name.

5-Sekunden-Regel



Nehmen Sie sich 5 Sekunden Zeit und prüfen Sie jede Überweisung genau – es kann Ihr Geld schützen!

5 Regeln für sichere Überweisungen



Persönlich bestätigen

Bei Änderungen der Bankverbindung immer telefonisch oder persönlich bestätigen.



Schützen Sie Ihre Daten

Geben Sie Bankdaten nie weiter und klicken Sie nicht auf Links in E-Mails oder Nachrichten.



Misstrauisch sein

Seien Sie skeptisch bei ungewöhnlichen Anfragen, Zeitdruck oder unbekannten Absendern.



Belege aufbewahren

Speichern Sie Rechnungen, E-Mails und Überweisungsbelege sorgfältig.



Im Zweifel fragen

Fragen Sie bei Unsicherheit Ihre Bank, Vertrauenspersonen oder Kollegen.



Wichtig!

Überweisungen sind in der Regel nicht rückgängig zu machen.
Vorsicht schützt vor Verlust!



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

QR-Rechnung – einfach, schnell, sicher

Die QR-Rechnung macht Überweisungen einfacher und sicherer.

Scannen, prüfen, bezahlen – fertig!

Was ist eine QR-Rechnung?

Die QR-Rechnung enthält alle Zahlungsinformationen in einem QR-Code.

Sie brauchen nur noch den Code zu scannen – Ihre Banking-App übernimmt den Rest.

Ihre Vorteile



Weniger Tippfehler

Alle Daten werden automatisch übernommen.



Schneller bezahlen

Scannen statt Abtippen – spart Zeit und Nerven.



Sicherer

Standardisiert und geprüft – für mehr Sicherheit.



Umweltfreundlich

Weniger Papier, weniger Aufwand – gut für die Umwelt.

So sieht eine QR-Rechnung aus

Rechnung

Nr. 2026-05-1234

Rechnungsdatum: 12.05.2026

Rechnung an:
Max Mustermann
Musterstraße 12
12345 Musterstadt

Beschreibung	Betrag
Dienstleistung / Lieferung	250,00 EUR
Summe	250,00 EUR

Zahlungsempfänger:
Muster GmbH
Beispielweg 1
54321 Beispielstadt
IBAN: DE12 3456 7890 1234 5678 90

Zahlbar bis: 26.05.2026


Zahlen mit Code





Tipp: Viele Banking-Apps finden den QR-Scanner direkt auf der Startseite oder im Menü „Überweisen“.



Vorsicht bei QR-Codes von Unbekannten!

Scannen Sie QR-Codes nur von vertrauenswürdigen Absendern. Betrüger können falsche QR-Codes versenden.

5 Schritte zur Zahlung mit QR-Rechnung

1



QR-Code scannen

Öffnen Sie Ihre Banking-App und scannen Sie den QR-Code.

2



Daten prüfen

Prüfen Sie Empfänger, IBAN und Betrag sorgfältig.

3



Verwendungszweck prüfen

Überprüfen oder ergänzen Sie den Verwendungszweck, falls nötig.

4



Zahlung freigeben

Bestätigen Sie die Zahlung in der App mit Ihrer gewohnten Freigabe (z. B. TAN, Face ID, Fingerabdruck).

5



Bestätigung erhalten

Sie erhalten sofort eine Bestätigung Ihrer Zahlung.



Wichtig zu wissen

Eine QR-Rechnung kann nur einmal bezahlt werden. Bewahren Sie Rechnungen auf – als Nachweis für Ihre Zahlung.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Apple Pay & Google Pay – mit dem Smartphone bezahlen



Achten Sie auf das
Kontaktlos-Symbol
am Terminal oder an der Kasse.

Kontaktlos, schnell und sicher – überall dort, wo Sie dieses Symbol sehen.

Einfach entsperren, ans Terminal halten, bestätigen – fertig!

Was sind Apple Pay & Google Pay?



Apple Pay (iPhone, Apple Watch) ist ein Bezahlservice von Apple. Ihre Kartendaten werden sicher im Gerät gespeichert – nicht auf Apple-Servern.



Google Pay (Android-Smartphones, Wear OS) ist ein Bezahlservice von Google. Ihre Kartendaten werden sicher im Gerät gespeichert – nicht auf Google-Servern.

Ihre Vorteile



Schnell: Keine Karte suchen – Smartphone entsperren, ans Terminal halten – fertig.



Sicher: Ihre echten Kartendaten werden nicht übertragen. Stattdessen wird ein verschlüsselter Code (Token) genutzt.



Einfach: Funktioniert in Geschäften, Restaurants, Tankstellen, Apps und online.



Überall akzeptiert: Dort, wo kontaktlose Zahlungen möglich sind – in Deutschland und weltweit.



Vergleich zur kontaktlosen Karte

Apple Pay und Google Pay funktionieren wie Ihre kontaktlose Bankkarte – nur digital. Statt Ihrer Karte nutzen Sie Ihr Smartphone oder Ihre Uhr.



Funktioniert überall, wo kontaktlose Zahlungen möglich sind.



Gleiche Sicherheit wie bei Ihrer Karte – dank modernster Verschlüsselung.



Weltweit nutzbar – überall, wo das Kontaktlos-Symbol zu sehen ist.

So bezahlen Sie – in 4 einfachen Schritten

1 Gerät entsperren

Entsperren Sie Ihr Smartphone oder Ihre Smartwatch mit Face ID, Touch ID, Fingerabdruck oder PIN/Passwort.

iPhone



oder



Android-Smartphone



oder

Wear OS Uhr



2 An das Terminal halten

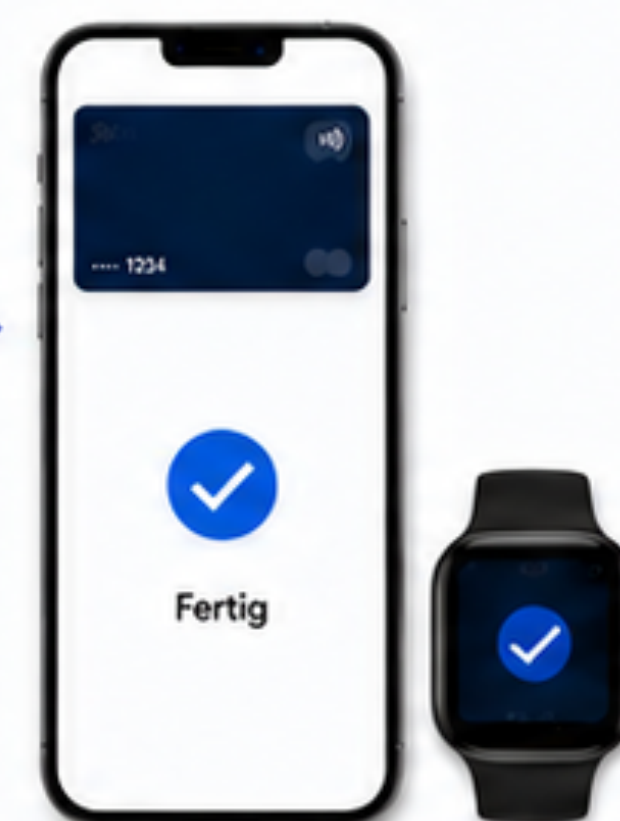
Halten Sie die Rückseite des Smartphones oder die Uhr nah an das Kontaktlos-Symbol des Terminals.



Tipp: Einige Sekunden halten, bis die Bestätigung angezeigt wird und ein Signal ertönt.

3 Zahlung bestätigen

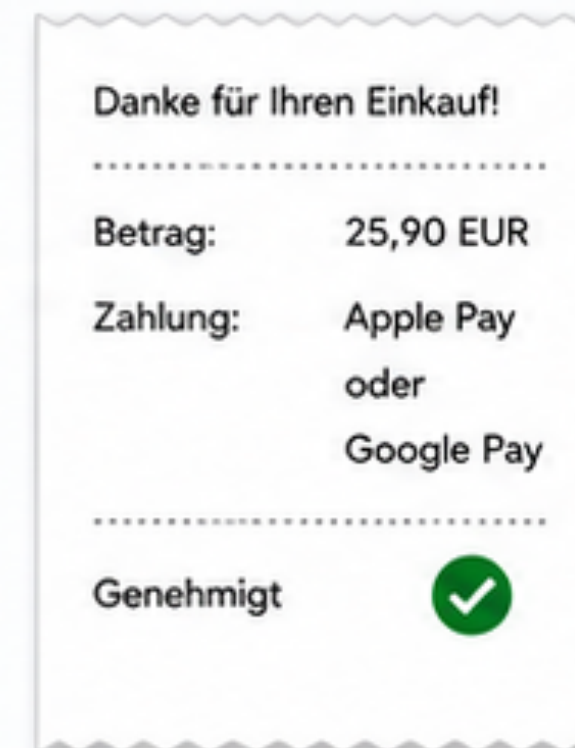
Bestätigen Sie die Zahlung mit Face ID, Fingerabdruck, PIN oder Ihrer Uhr – je nach Gerät.



Ein Signal oder eine Meldung bestätigt die erfolgreiche Zahlung.

4 Beleg erhalten

Sie erhalten wie gewohnt Ihren Kassenbon – auf Papier oder digital.



Den Beleg können Sie wie gewohnt aufbewahren – digital oder auf Papier.



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam

Ihre Sicherheit steht an erster Stelle



Keine echten Kartendaten werden gespeichert oder übertragen.



Jede Zahlung wird verschlüsselt und mit einem einmaligen Code (Token) durchgeführt.



Bei Verlust können Sie Ihr Gerät sofort sperren – dann können keine Zahlungen mehr erfolgen.



Sie erhalten eine Mitteilung nach jeder Zahlung (falls von Ihrer Bank angeboten).

Das Wallet – Ihre digitale Brieftasche

Im Wallet (auch Geldbörse genannt) bewahren Sie digitale Karten, Tickets und Pässe sicher an einem Ort auf – immer dabei auf Ihrem Smartphone oder Ihrer Smartwatch.

Alles Wichtige. Immer griffbereit.

Was ist ein Wallet?



Ein Wallet ist eine App auf Ihrem Gerät, in der Sie digitale Karten und Tickets speichern. Sie haben alles Wichtige dabei – statt vieler Plastikkarten und Papierbelege.

Das können Sie im Wallet speichern



Zahlungskarten

Debitkarten, Kreditkarten, Prepaidkarten (z. B. für Apple Pay / Google Pay)



Kundenkarten & Treueprogramme

Punkte sammeln und Vorteile nutzen



Tickets

Veranstaltungen, Kino, Konzerte, Sport und vieles mehr



Reise & Mobilität

Bordkarten, Bahnfahrkarten, ÖPNV-Tickets, Mietwagen, Parktickets



Ausweise & Pässe (je nach Land/Anbieter)

z. B. Führerschein, Studentenausweis, Impfpass (digitale Nachweise)



Gut zu wissen

Nicht alles ist überall verfügbar. Welche Karten, Tickets oder Ausweise unterstützt werden, hängt von Ihrem Land, Ihrer Bank und dem Anbieter ab. Fragen Sie bei Ihrer Bank oder beim Anbieter nach, wenn Sie etwas im Wallet speichern möchten.

Zwei Wallets – ein Ziel: alles Wichtige dabei



Apple Wallet

(iPhone, Apple Watch)

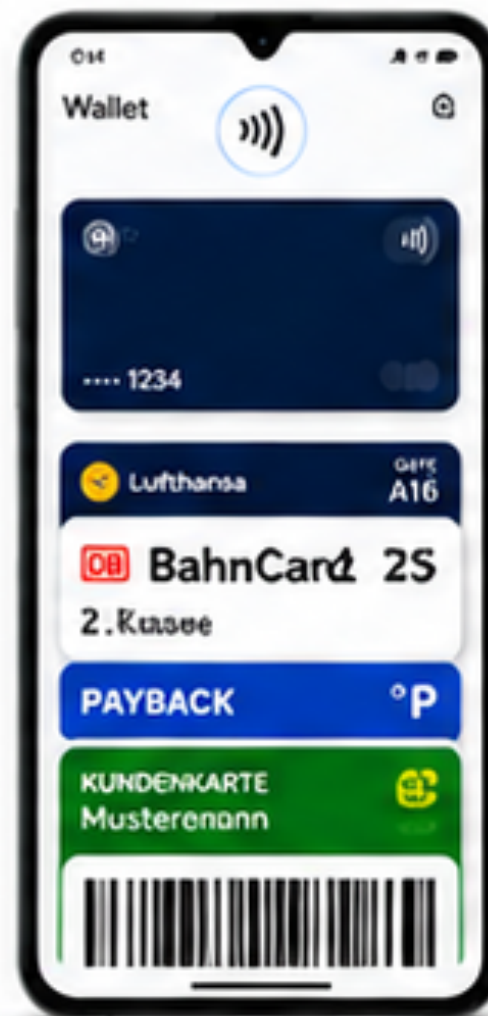
- ✓ Integriert auf allen iPhone und Apple Watch Geräten
- ✓ Für Apple Pay, Karten, Tickets, Pässe und mehr
- ✓ Sicher durch Apple-Technologie und Geräteverschlüsselung



Google Wallet

(Android-Smartphones, Wear OS)

- ✓ Auf Android-Smartphones und Wear OS-Smartwatches
- ✓ Für Google Pay, Karten, Tickets, Pässe und mehr
- ✓ Sicher durch Google-Technologie und Geräteschutz



So kommt etwas ins Wallet



Von Ihrer Bank

Karte hinzufügen – direkt in der Banking-App oder im Wallet.



Automatisch

Bei einigen Zahlungen oder Buchungen wird die Karte oder das Ticket automatisch angeboten.



Per QR-Code

QR-Code scannen und Karte oder Ticket wird ins Wallet übernommen.



Aus E-Mails oder Apps

Viele Anbieter bieten „Zu Wallet hinzufügen“ – mit einem Tipp gespeichert.



Manuell hinzufügen

Karten- oder Ticketdetails eingeben und speichern.



Tipp: Halten Sie Ihr Wallet aktuell.

Entfernen Sie Karten oder Tickets, die Sie nicht mehr benötigen.

Ihre Vorteile



Immer dabei

Alles Wichtige in Ihrem Smartphone oder Ihrer Smartwatch.



Schnell verfügbar

Mit einem Blick oder Tipp haben Sie, was Sie brauchen.



Sicher gespeichert

Ihre Daten sind verschlüsselt und gut geschützt.



Weniger ist mehr

Weniger Karten und Papier – besser für die Umwelt.



Tickets immer aktuell

Aktualisierungen (z. B. neue Uhrzeit oder Gate) werden automatisch übernommen.



Wichtig zu wissen

- Das Wallet speichert Ihre Daten sicher – nicht auf Karten oder Papier.
- Bei Verlust sperren Sie Ihr Gerät sofort über „Mein Gerät finden“.
- Für Zahlungen benötigen Sie Ihre Entsperrung (Face ID, Touch ID, PIN oder Muster).



Gefördert durch die
Gemeinde Rangsdorf



**Smartphone-
Sprechstunde**



Referent:
Martin Adam