Volksbank
Darmstadt Mainz

OnlineBanking sicher nutzen – Betrügern keine Chance geben

Vortrag 21.10.2025 um 16:00 Uhr Gau-Algesheim

Volksbank Darmstadt Mainz

Agenda

1. **Herzlich Willkommen**
2. **Einstieg ins OnlineBanking**
   a. Überblick/Funktion OnlineBanking
   b. TAN-Verfahren
   c. elektronisches Postfach
   d. Möglichkeiten & Serviceaufträge
   e. Live-Präsentation
3. **Betrugsprävention**
   a. häufige Betrugsmaschen
   b. erste Hilfe
   c. Tips & seriöse Hilfestellung Online
4. **Ihre Fragen**

Volksbank
Darmstadt Mainz

Maren
Kraus

Produktmanagerin Banking & Payments Cyber Security

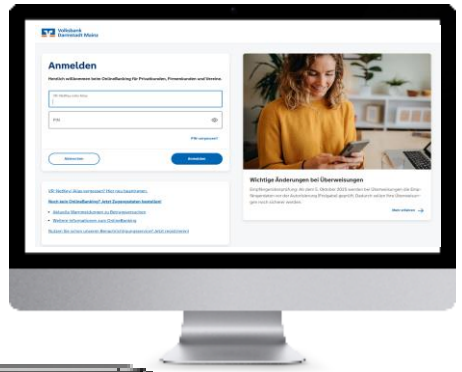
maren.kraus@volksbanking.de
06131-148 4848

- Seit 01.10.2012 bei der Volksbank, 49 Jahre alt, verheiratet, 2 erwachsene Söhne
- Vorherige Tätigkeiten: Kunden & Anlageberatung, KDC, Business-Banking
- Berufliche Leidenschaften:
  Alles rund um das Thema OnlineBanking & Digitalisierung
  Interaktion & Kommunikation mit unseren Kunden
  Betrugsprävention & Fraud Management

Volksbank Darmstadt Mainz

OnlineBanking sicher nutzen

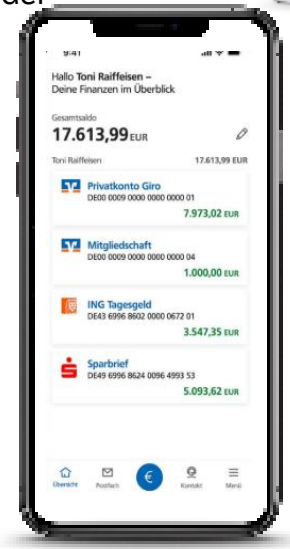
Online-Banking bei der Volksbank Darmstadt Mainz eG



Abwicklung von Bankgeschäften online

Voraussetzung

- Aktive Geschäftsbeziehung oder Vollmacht für ein Kundenkonto
- internetfähiges Gerät (Handy, PC, Laptop, Tablet) & Internetzugang (für Nutzung der Apps Anforderung Betriebssystem mind. Android 9 oder iOS 16.7)
- Nutzung eines gesicherten Netzwerkes!



Benötigte Unterlagen

- Kundenstammvertrag bzw. Vereinbarung über die Nutzung des Onlinebankings
- VR-NetKey
- Persönlich Identifikationsnummer (PIN)
- TAN-Verfahren, zur Freigabe der Aufträge

Volksbank Darmstadt Mainz

Zugangswege/ Zugangsdaten

Sie erhalten von uns:

- Der **VR NetKey** ist Ihre persönliche Benutzerkennung bestehend aus einer Zahlenfolge (zusätzlich Anlage eines ALIAS möglich)
- **PIN** = persönliche Identifikationsnummer - diese erhalten Sie als 8stellige Nummer und müssen diese bei der ersten Nutzung in eine persönliche PIN oder ein Passwort abändern
- Aktuell bieten wir 2 unterschiedliche **TAN-Verfahren** an:

1. VR SecureGoPlus App – FreigabeApp auf dem Handy
2. Sm@rt-TAN – separates Gerät/TAN-Generator mit girocard

- **Diese 3 Komponenten benötigen Sie für die Anmeldung im OnlineBanking. Bei PIN/Passwort und TAN-Verfahren handelt es sich um sensible Autorisierungsdaten! Bitte verwenden Sie diese nur zu Anmeldung auf unseren OnlineBanking-Plattformen! Wir werden Sie niemals die Herausgabe dieser Daten von Ihnen verlangen.**

Volksbank Darmstadt Mainz

VR NetKey

- Persönliche Benutzerkennung bestehend aus einer Zahlenfolge (zusätzlich Anlage eines ALIAS durch Kunden möglich)
- Anmeldung über VR-NetKey kann für folgende „Plattformen“ genutzt werden:
  - OnlineBanking über die Homepage (PC oder mobiles Endgerät)
  - VR-Banking App und Apps von Drittanbietern
  - Software-Produkte
  - Verbundseiten
  - Telefonbanking (PIN muss rein nummerisch sein)
- PIN-Fehlversuche:
  - Sperre erfolgt ab der 3. Falscheingabe
  - Kunde kann sich mit korrekter PIN und TAN- bzw. Sicherheitsverfahren selbst freischalten
  - ab dem 9. Fehlversuch wird eine neue PIN erstellt und per Post zugeschickt

Ein VRNK pro Kunde!

Regeln für die neue PIN:

Mindestens 8, maximal 20 Stellen.
Die PIN muss entweder rein numerisch sein oder mindestens einen Großbuchstaben und eine Ziffer enthalten.
Verwenden Sie keine leicht zu erratende PIN, wie zum Beispiel Zahlenfolgen oder zu einfache Zahlen- und Zeichenkombinationen.
Erlaubter Zeichensatz:
Buchstaben (a-z und A-Z, inkl. Umlaute und ß)
Ziffern (0-9)
Die Sonderzeichen @!%&/=?*+;:,._-
Falls Sie iOS nutzen, beachten Sie bitte, dass Sonderzeichen in der PIN-Eingabe blockiert werden können, insbesondere wenn Ihre PIN Zeichen wie '...' oder einen doppelten Bindestrich enthält.

VR SecureGo Plus App

Vorteile im Überblick

kostenfrei !

- Authentifikation jederzeit sicher und bequem per Smartphone
- Nur eine App für OnlineBanking-Transaktionen und Kreditkarten-Zahlungen nötig
- Einfache und schnelle Online-Registrierung mithilfe eines QR-Codes zur Aktivierung
- Aktivierungscode erhalten Kunden auf dem Postweg oder direkt in der Filiale
- Direktfreigabe-Funktion zur schnellen und einfachen Ausführung von Zahlungsaufträgen innerhalb der App (kein Wechsel und keine manuelle Eingabe von TAN mehr erforderlich)
- Hohe, durch den TÜV Saarland geprüfte Sicherheitsstandards
- Einrichtung und Nutzung auf maximal drei Geräten gleichzeitig
- nach 3maliger Fehleingabe des Freigabecodes sperrt sich die App für weitere TAN-Freigaben. Einen Entsperrcode erhalten Sie automatisch auf dem Postweg

TÜV SAARLAND Geprüfte App Produktprüfung
tuev-saar.de/TK45294

Nutzung der VR SecureGo plus

Und so nutzen Sie VR SecureGo plus

1. Geben Sie Ihren Auftrag im OnlineBanking ein.
Sie erhalten automatisch eine Push-Nachricht auf Ihrem mobilen Gerät.

2. Öffnen Sie die App.
Wechseln Sie zu VR SecureGo plus und prüfen Sie die Auftragsdaten.

3. Geben Sie Ihren Auftrag frei.
Mit Ihrem individuellen Freigabe-Code, Ihrem Fingerabdruck oder der Gesichtserkennung geben Sie den Auftrag frei. Alternativ tragen Sie die angezeigte TAN in Ihrem OnlineBanking ein.

4. Auftrag wird bestätigt.
Sie erhalten in der App einen Verarbeitungshinweis. Prüfen Sie im OnlineBanking die erfolgreiche Ausführung Ihres Auftrags.

Volksbank Darmstadt Mainz

Sm@rt-TAN-Verfahren

Vorgehensweise

- Sie arbeiten mit einem TAN-Generator und Ihrer girocard
- Es kann nur eine girocard für das Verfahren zugeordnet werden – die TAN-Erzeugung erfolgt unabhängig vom Konto, von dem die Überweisung getätigt wird!
- Je nach Gerätetyp unterschiedliche Vorgehensweisen zur TAN-Erzeugung:
  - optische Methode mit Sm@rt TAN photo
  - manuelle Methode mit Eingaben über den TAN-Generator
- Banken und Sparkassen nutzen hier mittlerweile ihre ganz eigenen Verfahren und Geräte (hybride Geräte nur teilweise erhältlich)
- TAN-Generator kann von den Kunden über www.volksbanking.de/shop bestellt werden – Kosten Hybridgerät 22,99 €

Entsperrung nach Fehlversuchen (3malige Falscheingabe)

- nach 3maliger Fehleingabe der TAN sperrt sich das TAN-Verfahren aus Sicherheitsgründen, eine Rücksetzung der Sperre erfolgt gemeinsam mit einem Mitarbeiter der Volksbank

Volksbank Darmstadt Mainz

Verwendung des Sm@rt-TAN photo Generators

1

Richtige Karte in den TAN-Generator stecken

2

Code abscannen

3

Bestätigung mit OK

4

TAN-Eingabe

Volksbank Darmstadt Mainz

Elektronisches Postfach

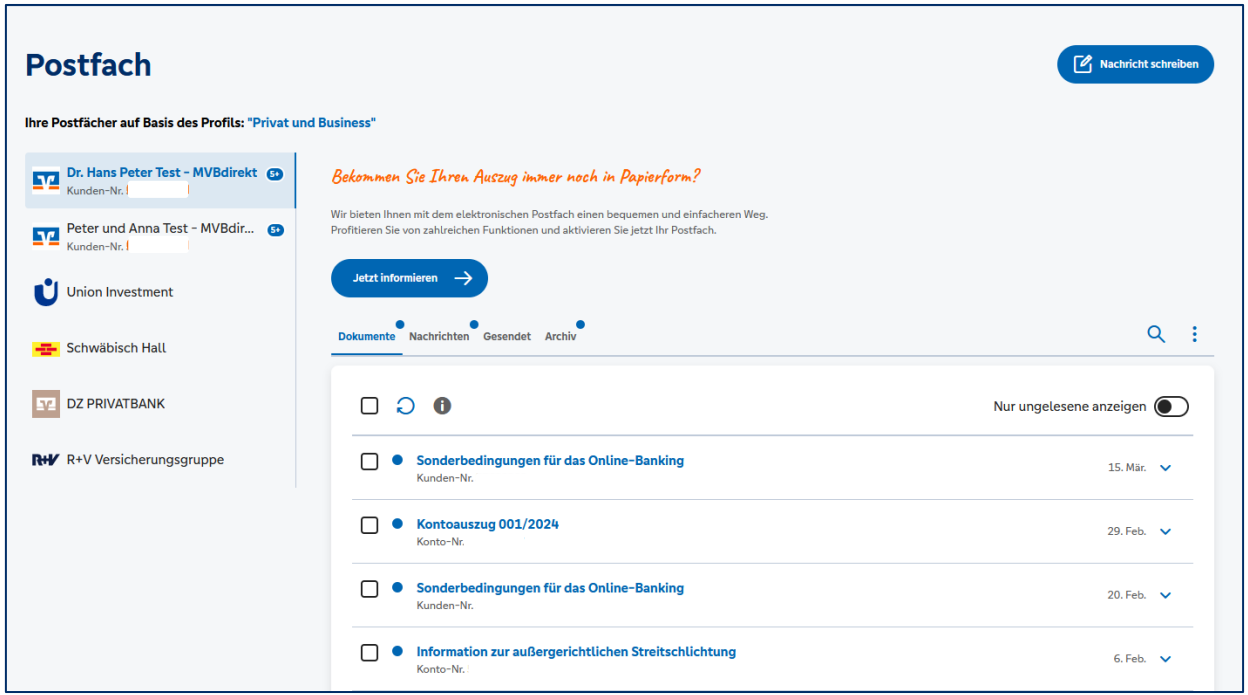
Funktionsweise

- Sowohl im OnlineBanking als auch in der VR Banking App (bei der Erstbankverbindung) nutzbar
- Aktuelle Dokumente jederzeit und überall abrufen, archivieren (bis zu 10 Jahre!) und ausdrucken:
  - Kontoauszüge
  - Kreditkartenabrechnungen
  - Wertpapierdokumente
  - Vertragsunterlagen; AGB-Änderungen
- Verbundpostfächer (Union, BSH, R+V usw.)
- Sichere Kommunikation mit uns durch TAN-gesicherte Nachrichten
- Ablage der Dokumente nach Personennummer
- Filtermöglichkeiten und Suchfunktion
- Je nach Kontomodell Standard bzw. Voraussetzung
- Kunden können sich dafür selbst im ePostfach im OnlineBanking freischalten

Digitales Postfach für den Kunden

Unterlagen in digitaler Ausfertigung rund um das Konto

- Kontoauszüge
- Kreditkartenabrechnungen
- Wertpapierdokumente
- Vertragsunterlagen
- Änderungen der AGB
- Verbundpostfächer



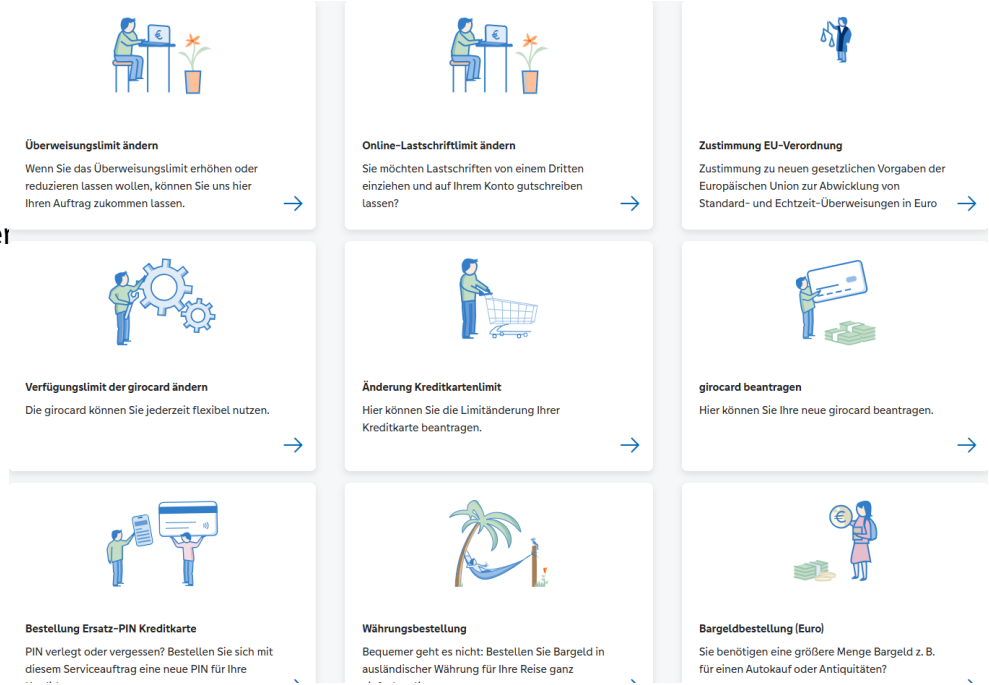
Volksbank Darmstadt Mainz

Beliebte Funktionen im Überblick

Neben den Standardfunktonen wie z. B. Konten- und Umsatzanzeige, Überweisungen, Daueraufträge etc:

- Multibankenfähigkeit – Integration Konten von Fremdbanken
- Chat mit einem unserer Mitarbeiter
- elektronisches Postfach
- Rückrufwunsch anmelden
- Aktien im Depot und Fonds im UnionDepot verwalten
- Börse und Aktienmärkte im Blick behalten
- Kartenverwaltung incl. Digitalisierung
- Prepaid-Guthaben fürs Handy aufladen
- Limitsteuerung für das Banking und Karten
- Währungen bestellen
- Ersatzauszüge bestellen
- Steuerbescheinigungen anfordern
- Benachrichtigungsservice

Neu: wero



Online-Banking inkl. Live Demo

Volksbank Darmstadt Mainz

Betrügern keine Chance geben

Betrugsmaschen

Finanzagenten

Betrug an Geldautomaten

Falsche Bank-Mitarbeiter

Anlagebetrug

Betrug durch falsche Polizisten

Warenbetrug

Falsche Paypal-Mitarbeiter

giro- und Kreditkartenbetrug

Gewinnversprechen

Fake-Shops

Betrug mit Wohnungsangeboten

Falsche Microsoft-Mitarbeiter

Love-Scamming

Enkeltrick

Bestellbetrug

Haustürbetrug

Social Engineering

Volksbank Darmstadt Mainz

Enkeltrick & WhatsAppBetrug

Hallo Mama, das ist meine neue Handynummer. 0157-47110815 Bitte speichern und schreib mir eine SMS.

Hallo Papa, ich bin in Schwierigkeiten. Bitte überweise mir dringend 500,- Euro an mein Konto: LT23REV765429888825. Danke.

Hallo Oma, weisst Du wer hier ist? Genau, Dein Enkel. Ich habe einen Unfall versursacht und brauche dringend Geld um nicht verhaftet zu werden... Bitte erzähl niemandem davon, dass ich in Schwierigkeiten bin!!!

Oma macht sich auf den Weg zur Bank....

- Angreifer spielen mit dem Schockmoment der Adressaten oder erpressen emotional, daher wird das rationale Denken quasi ausgeschaltet.
- klassisch per Telefonanruf oder SMS/WhatsApp, Schockanrufe auch mit Unfallszenarien oder Anrufe falscher Polizisten
- niemals am Telefon Bankdaten oder Autorisierungsdaten herausgeben
- Einfach Auflegen und Nachrichten löschen, bei Unsicherheit direkten Kontakt auf den altbekannten Nummern suchen und nicht über die Nummer von der angerufen wurde oder die angeblich neu ist!

Anlagebetrug: Vorsicht bei lukrativen Geldgeschäften ohne Risiko!

Mit falschen Versprechen, über einfache Kapitalanlagen mit hohen Renditen, locken private Kreditvermittler und unseriöse Anlageberater arglose Kunden.

Beim **Anlagebetrug** wird oft gezielt mit falschen oder unwahren Angaben zu Renditen und Risiken geworben. Manchmal werden hohe Gewinne vorgegaukelt, indem im **Schneeballsystem** Gelder eines Investors zur Zahlung von Renditen eines anderen Investors genutzt werden. Der Schwindel fällt dann erst auf, wenn das Schneeballsystem zusammenbricht oder die Kunden selbst auch gar nicht mehr in ihr neues OnlineBanking kommen, um ihre Anlage zu überprüfen. Die Gelder werden meist ins Ausland transferiert, bitte prüfen Sie Zahlungen nach Malta, ins Baltikum, England & Irland sowie Frankreich sehr genau und fragen bei unseren Kundinnen und Kunden nach dem Hintergrund der Zahlung.

Der Kontakt kommt oftmals per Social Media und Onlinewerbung zustande und Kunden werden in Chats kontaktiert und geködert.

Anlagebetrug: Vorsicht bei lukrativen Geldgeschäften ohne Risiko!

Das sollten Sie wissen:

- Ungewöhnlich hohe Gewinne mit wenig Einsatz, sollten immer misstrauisch machen.
- Seien Sie misstrauisch, wenn die Investitionen in Kryptowährungen getätigt werden sollen.
- Banken und Sparkassen gehen nicht direkt auf Kunden zu, um sie zum Online-Trading zu bringen.
- Informieren Sie sich über die Trading-Plattformen, bevor Sie sich anmelden oder Geld überweisen. - Nutzen Sie dafür z. B. die Unternehmensdatenbank der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht)
- Lassen Sie sich nicht unter Druck setzen. Fragen Sie notfalls bei der offiziellen Plattform nach, wer der Händler ist.
- Geben Sie keine sensiblen Daten preis, wie Zugangsdaten zum Online-Banking oder zum Depot, Ausweisfotos oder Ihre Anschrift.
- Überweisen Sie kein Geld auf unbekannte Konten.

Befürchten Sie Opfer geworden zu sein? Erstatten Sie Anzeige bei Ihrer örtlichen Polizei und melden es bei Ihrer Bank!

Telefonbetrug: Angeblicher Bankmitarbeiter oder Servicemitarbeiter

Derzeit werden Kunden auch wieder vermehrt von **angeblichen Bankmitarbeitern** oder der **Sicherheitsabteilung** unserer Bank angerufen und im Gesprächsverlauf

- zur Herausgabe von Online Banking-Zugangsdaten aufgefordert
- unter Vorgabe falscher Tatsachen zur Durchführung einer Überweisung aufgefordert (z.B. angeblich zur Rücküberweisung eines falschen Geldeingangs, zur Vorschusszahlung für einen Kredit oder aufgrund eines Sicherheitsvorfalls)
- oder es wird ihnen ein (nicht vorhandener) Geldausgang suggeriert, so dass der Angerufene die Zahlung stornieren möchte. In diesen Fällen haben die Betrügenden bereits im Vorfeld die VR Netkey-Daten abgegriffen.

Auf dem Display des Telefons erscheint die Nummer unserer Bank, welche aber mithilfe technischer Möglichkeiten der Rufnummernanzeige dem Angerufenen vorgetäuscht wird.

Hinweis: Solche Anrufe können auch durch einen angeblichen „Microsoft-Mitarbeiter, PayPal-Mitarbeiter, bzw. von vielen verschiedenen KundenServiceCenter erfolgen.

Love-Scamming: Betrug mit vorgetäuschter Liebe

In **Online-Partnerbörsen** oder auch in **sozialen Netzwerken** sind die Scammer auf der Suche nach potenziellen Opfern. Ist ein Kontakt erst einmal hergestellt, werden diese mit Liebesbekundungen und Aufmerksamkeit überhäuft – und zwar einzig und allein mit dem Ziel, ihnen das Geld aus der Tasche zu ziehen.

Vorgehensweise der Täter

- Betrüger machen sich im täglichen Leben der Opfer unverzichtbar
- Romantische Mails ein kurzes Telefonat um eine Emotionale Bindung aufzubauen
- Schöne Fotos werden dem Opfer geschickt
- Erfragen persönliche Dinge und täuschen ein sehr großes Interesse vor
- Geld wird für den Flug, Hotel, Visum oder Transfer benötigt
- Immer eine Ausrede, warum das Ticket oder der Flug nicht wahrgenommen werden konnten
- Grundsätzlich sollte man Menschen, die man nie persönlich kennengelernt oder gesehen hat, kein Geld überweisen oder auf sonstige Forderungen eingehen. Gerade im Internet tummeln sich viele **Betrüger, die an der Gutgläubigkeit ihrer Mitmenschen viel Geld verdienen** wollen. Seien Sie also immer **misstrauisch bei unglaublichen Angeboten**, ob bei der Wohnungs- oder der Partnersuche.

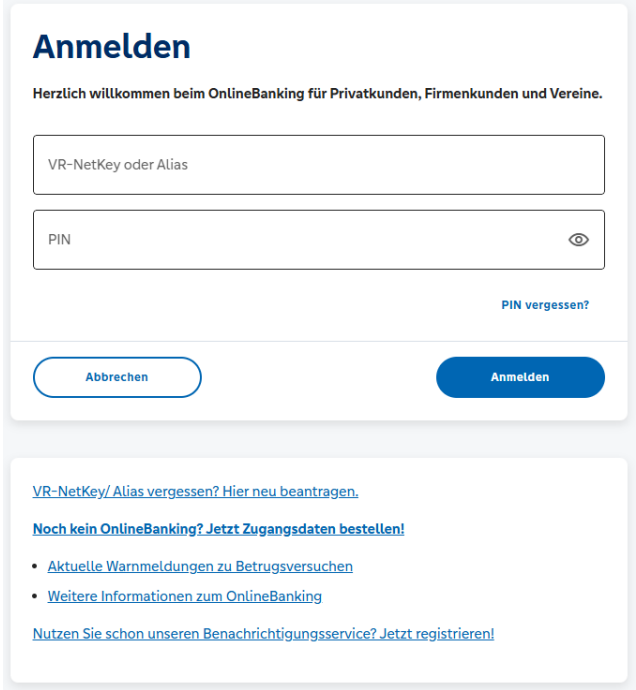
Sofortmaßnahmen bei Betrugsverdacht & Phishing für Kunden

- Bewahren Sie Ruhe und versuchen Sie für sich nachzuvollziehen was passiert ist und überlegen Sie ob Zugangsdaten, Karten oder Legitimationsdaten in falsche Hände geraten sind/sein können.
- Gibt es unklare oder betrügerische Buchungen auf dem Konto?
- Nehmen Sie umgehend Kontakt zu Ihrer Bank auf!
  Volksbank Darmstadt Mainz eG auf 06131-148 8000
- Außerhalb unserer Servicezeiten:
  - **Sperren Sie Ihre Karten und/oder das OnlineBanking über den Sperrnotruf 116 116** Über diese Nummer können Sie girocard, Mastercard und Visa Karte sowie digitale Karten und Ihr OnlineBanking sperren.
    (Aus dem Ausland +49 116 116 oder +49 30 40 50 40 50)
  - Es gibt auch eine Sperr-App fürs Handy „116 116 Sperr-App“ im App/Playstore!
  - Bitte im Nachgang dann Kontakt mit Ihrer Bank aufnehmen.
- Ist ein Zahlungsverkehrsdienstleister (z.B. Paypal) betroffen? Bitte direkt an den Support des Anbieters wenden.
- Sichern Sie eventuelle Beweise und erstatten Sie Anzeige bei der Polizei. Dies ist auch online möglich
- **Im Zweifel direkt Karten und Onlinezugang sperren, damit gar nicht erst ein Schaden entstehen kann!**

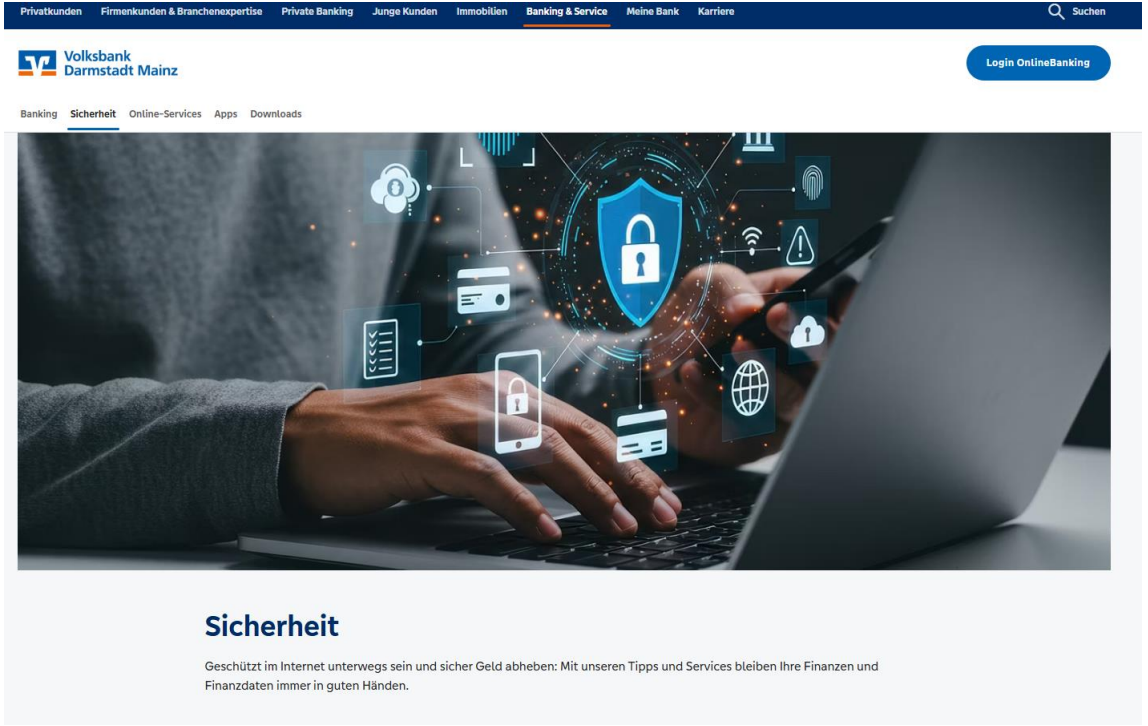
Aktuelle Phishing-Warnungen

finden Sie auch auf unserer Homepage www.volksbanking.de

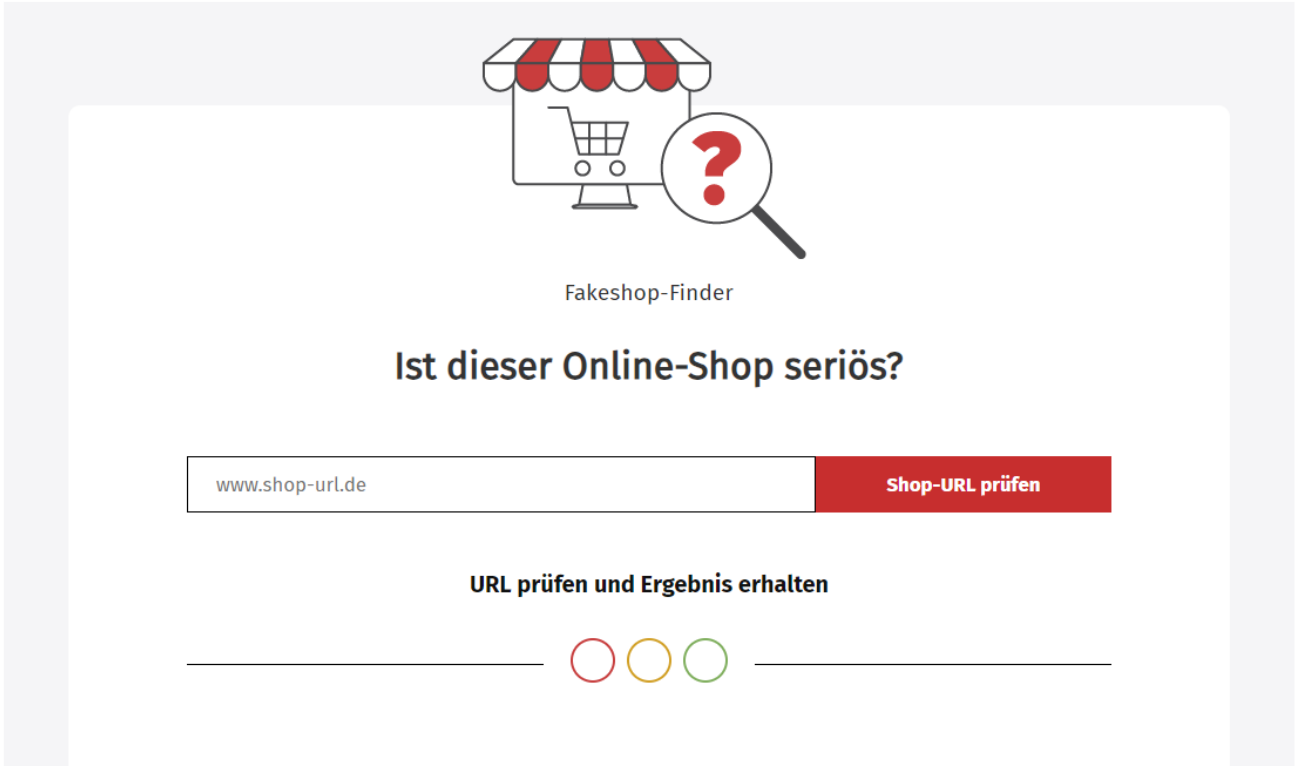
z.B. im LogIn Bereich des OnlineBankings



oder unter ‚Banking&Service' im Reiter ‚Sicherheit'



Fakeshop-Finder: Prüfen Sie, ob ein Online-Shop seriös ist | Verbraucherzentrale.de



Nutzen Sie unseren Sicherheitscheck

www.volksbanking.de/sicherheitscheck

- auf unserer Homepage integriert
- bietet die Möglichkeit zur Überprüfung der Nutzungsgewohnheiten im Onlinebanking und Reflektion zum Thema Sicherheit im Onlinebanking bzw. Internet
- Hinweise und Tips zum Umgang mit der genutzten Soft-/Hardware
- Einfache Klickstrecke von 8 Fragen, die man schnell beantworten kann.
- Man erhält eine pdf-Auswertung mit wertvollen Tipps und Hinweisen. Diese können Sie für sich verwenden oder auch an uns übermitteln wenn es noch weitere Fragen gibt. Wir beraten dann gerne weiterführend!

www.polizei-beratung.de

Wir wollen, dass Sie sicher leben. Ihre Polizei

POLIZEILICHE KRIMINALPRÄVENTION
DER LÄNDER UND DES BUNDES

Suche nach Themen, Tipps und Hilfe

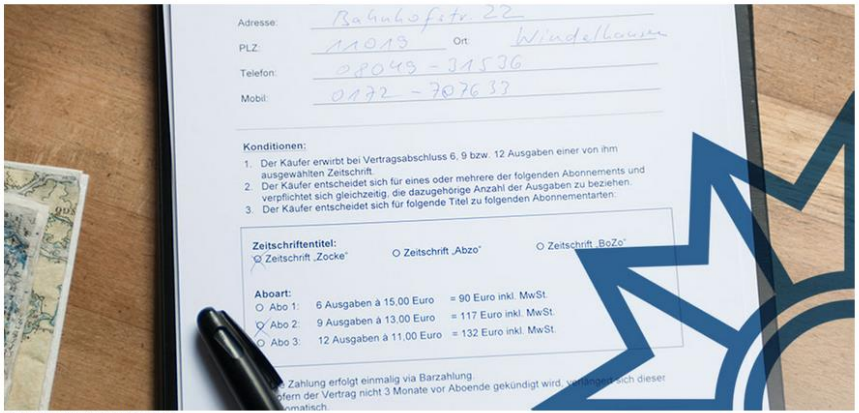
Themen & Tipps | Infos für Betroffene | Medienangebot | Presse | Newsletter

Themen & Tipps > Betrug

BETRUG

- Arzneimittel
- Bestellbetrug
- Betrug an Geldautomaten
- Betrug durch falsche Polizisten
- Betrug im Urlaub
- EC- und Kreditkartenbetrug
- Enkeltrick
- Falsche Microsoft-Mitarbeiter
- Falschgeld
- Finanzagenten
- Geldwäsche
- Gewinnversprechen
- Haustürbetrug
- Kredit- und Anlagebetrug
- Messenger-Betrug

Betrugsmaschen - Sie können sich schützen



© Polizeiliche Kriminalprävention

www.schufa.de

Einmeldung von Identitätsbetrug

durch Betroffene bei der SCHUFA

So funktioniert's:

1. Einwilligung und Formular vollständig ausfüllen und unterschreiben
2. Ausweisdokumente und Nachweis über die Erstattung einer Strafanzeige in Kopie beifügen
3. Vollständige Unterlagen per Post/Fax/E-Mail an uns senden

Wir senden Ihnen nach Aufnahme der Einmeldung eine Bestätigung

Wie Sie Identitätsbetrug bei der SCHUFA melden können

EINMELDUNG FÜR OPFER VON IDENTITÄTSBETRUG.

Bitte senden Sie das ausgefüllte Formular inklusive Kopien der erforderlichen Dokumente an:
SCHUFA Holding AG
Privatkunden ServiceCenter
Identitätsschutz
Postfach 103441
50474 Köln
Fax: 01805 - 910010 (14 Cent/Minute)
E-Mail: identitaetsschutz@schufa.de

Hiermit beantrage ich, dass meine persönlichen Daten als Identitätsbetrugsopfer zu meinem Schutz bei der SCHUFA gespeichert werden.

Zeit für Ihre Fragen

Volksbank Darmstadt Mainz

Fragen & Anliegen?

Unser Team Banking Cyber Security beantwortet Ihre Fragen.
Sie erreichen uns unter betrug@volksbanking.de