



Volksbank
Plochingen eG

»Hallo Oma,
ich brauch Geld!«



Herzlich
Willkommen!

Programmablauf

- Begrüßung
- Vorstellung unseres KundenDialogCenters
- Aktuelle Betrugsmaschen bei Zahlungssystemen
- Theaterstück “Hallo Oma, ich brauch Geld!”
- Fragen
- Verabschiedung



KundenDialogCenter



KundenDialogCenter
Beste Bankservice – persönlich, kompetent und schnell!

Ihr schnellster Draht zur Bank!
07153 706-0

The banner features the large letters 'KDC' in a dark blue font. The 'C' is stylized to resemble a telephone handset with signal waves. A white speech bubble contains the text 'KundenDialogCenter' and 'Beste Bankservice – persönlich, kompetent und schnell!'. An orange rounded rectangle contains the text 'Ihr schnellster Draht zur Bank!' and the phone number '07153 706-0'.

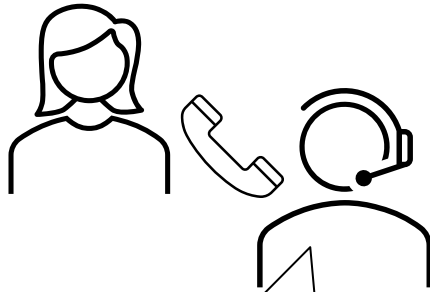
- Erreichbarkeit von Montag bis Freitag von 8 – 18 Uhr
- Dringende Angelegenheiten nicht auf die ‚lange Bank‘ schieben
- Persönliche Identifikation für ein hohes Maß an Sicherheit

KundenDialogCenter

- Konto-Service (Auskünfte / Überweisung / Dauerauftrag)
- Karten-Service (girocard / Kreditkarte)
- Online Banking-Service und Unterstützung
- Terminvereinbarung
- Weiterleitung an Fachspezialisten

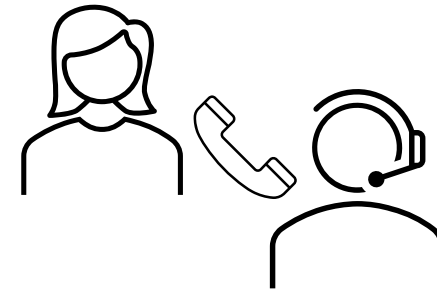


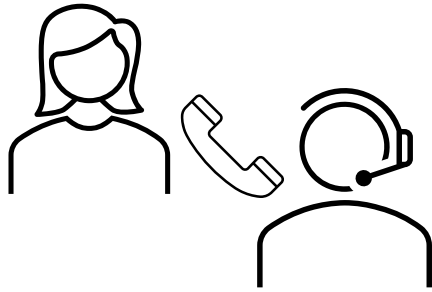




Vielen Dank.
Dafür müsste ich Sie einmal legitimieren.
Würden Sie mir hierzu bitte Ihren Namen, Ihr Geburtsdatum sowie die Adresse und Ihre Kartennummer nennen?

Ich heiße Martha Muster, bin am 01.01.1960 geboren und wohne Am Fischbrunnen 8 in Plochingen. Meine Kartennummer lautet 24003587552.





Vielen Dank, das passt.
Ihr aktueller Kontostand beträgt
150,50€. Kann ich sonst noch
etwas für Sie tun?



Danke, das wäre alles.
Auf Wiederhören.

Sehr gerne, ich wünsche
Ihnen einen schönen
Tag und bis zum
nächsten Mal.



Ihre Fragen zum KundenDialogCenter

Vielen Dank für Ihre Aufmerksamkeit

Volksbank Plochingen eG
Alisia Schüssler
Teamverantwortliche KundenDialogCenter
Am Fischbrunnen 8
73207 Plochingen
07153 706-0
email@volksbank-plochingen.de





Aktuelle Betrugsmaschen bei Zahlungssystemen

Betroffenheit der Bevölkerung in Zahlen, Daten, Fakten (06.2022 – 05.2023)

97.000 Opfer



Frankfurt:
760.000 Einwohner
920 Opfer/Erhebungszeitraum



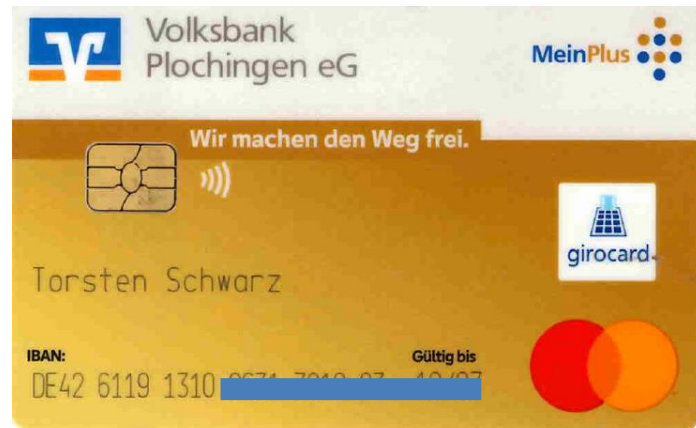
Unter 825 Einwohnern
ist ein 1 Opfer/Erhebungszeitraum



Es ist somit nicht eine Frage, ob Fraud passiert, sondern wann dieser eintritt!

Aktuelle Betrugsmaschen in Zahlungssystemen

PIN für die girocard oder die Kreditkarte



PIN girocard 1234

PIN kreditkarte 9876

PIN Handy 0000

Aktuelle Betrugsmaschen bei Zahlungssystemen

Geldwechseltrick vor dem Einkaufsladen



Aktuelle Betrugsmaschen bei Zahlungssystemen

Gefälschte Überweisungsbelege – Umgang mit persönlichen Daten

Überweisung GENODES1VBP

Volksbank Plochingen eG
73207 Plochingen, Am Fischbrunnen 8

Für Überweisungen in Deutschland, in andere EU-/EWR-Staaten, in das UK und die Schweiz in Euro. Kontoinhaber trägt Entgelte bei seinem Kreditinstitut; Zahlungsempfänger trägt die übrigen Entgelte.

Angaben zum Zahlungsempfänger: Name, Vorname/Firma (max. 27 Stellen, bei maschineller Beschriftung max. 35 Stellen)

BAUER MUELLER

IBAN DE 81 611 913 10 0699 9991 38

BIC des Kreditinstituts/Zahlungsdienstleisters (8 oder 11 Stellen) GENODES1VBP

Die Angabe des BIC kann bei Zahlungen innerhalb EU/EWR entfallen.

Betrag: Euro, Cent 123,56

Kunden-Referenznummer - Verwendungszweck, ggf. Name und Anschrift des Zahlers - (nur für Zahlungsempfänger)
MILCHGELD FÜR KUH ELSA
noch Verwendungszweck (insgesamt max. 2 Zeilen à 27 Stellen, bei maschineller Beschriftung max. 2 Zeilen à 35 Stellen)

Angaben zum Kontoinhaber: Name, Vorname/Firma, Ort (max. 27 Stellen, keine Straßen- oder Postfachangaben)
Torsten Schwarz

IBAN Prüfzahl Bankleitzahl des Kontoinhabers Kontonummer (rechtsbündig u. ggf. mit Nullen auffüllen)
DE 42 611 913 10 0631 301 003 16

Datum Unterschrift(en)

4/1.237 06.2023 (4/1.1437)

Aktuelle Betrugsmaschen bei Zahlungssystemen

Umgang mit persönlichen Daten

Bitte geben Sie auf telefonische Nachfrage, per E-Mail oder auf Internet-Seiten keine persönlichen Daten preis. Dazu gehört auch Ihre Kartenummer Ihrer girocard oder Kreditkarte.

Dies kann auch bei Kleinanzeigen.de vorkommen. Sie wollen etwas verkaufen und der Interessent erkundigt sich zur Zahlung nach Ihrer Kreditkartennummer. Hier ist Betrug im Spiel.

Aktuelle Betrugsmaschen bei Zahlungssystemen

Whatsapp - Betrug

Whatsapp-Betrug im vierstelligen Bereich

BISSINGEN. Ein Mann aus Bissingen ist am Mittwoch von unbekanntem Kriminellen betrogen worden. Wie die Polizei berichtet, flog der Betrug erst auf, als der Mann einen vierstelligen Betrag überwiesen hatte. Dem Angaben zufolge schrieben die Betrüger dem Mann zunächst eine Nachricht über den Messenger-Dienst Whatsapp. Der Absender gab sich als der Sohn des Geschädigten aus und forderte mehrere Überweisungen. Im Glauben, dass es sich tatsächlich um seinen Angehörigen handele, kam der Mann den Forderungen nach. Ob die Überweisungen von der Bank noch zurückgerufen werden können, steht noch nicht fest.

Die Polizei warnt in diesem Kontext. Bei Nachrichten von unbekanntem Nummern sollte stets Misstrauen geweckt werden und der angebliche Absender überprüft werden – insbesondere wenn Geldbeträge gefordert werden. Betrugsversuche sollen stets auch bei der Polizei angezeigt werden. *rko*

Esslinger Zeitung
vom 01.03.2024

Aktuelle Betrugsmaschen bei Zahlungssystemen

Whatsapp - Betrug

Film ab!

Aktuelle Betrugsmaschen bei Zahlungssystemen

Phishing

mit Phishing-Mails versuchen Betrüger, Sie per E-Mail unter falschem Vorwand zu einer Überweisung, zur Angabe Ihrer Zugangsdaten nicht nur zum Online-Banking oder zur Preisgabe Ihrer Kreditkartendaten zu verleiten. Es gibt viele Varianten – eines haben sie aber alle gemeinsam: Sie nutzen Vorwände, gefälschte Absenderadressen, Webseiten und Eingabemasken, die zum Beispiel einer Banking-Anwendung oder einer vertrauten Händlerseite täuschend ähnlich sehen.

Aktuelle Betrugsmaschen bei Zahlungssystemen

Vorgehensweise der Betrüger

Zunächst verschaffen sich die Betrüger Zugang zum Online-Banking, meistens durch Phishing. Damit registrieren sie ein eigenes Mobilgerät für VR-SecureGo plus. Anschließend fordern die Betrüger die Bankkunden in E-Mails, Telefonaten oder SMS auf, den versendeten Freischaltcode durchzugeben. Mithilfe des Freischaltcodes können die Betrüger den ein eigenes Gerät freischalten. Gleichzeitig löschen sie die Geräte der Bankkunden. Mit dem neu freigeschalteten Gerät führen sie dann Transaktionen durch, von denen die Bankkunden nichts mitbekommen.

Aktuelle Betrugsmaschen bei Zahlungssystemen

Aufruf zur Verlängerung der Legitimation für die VR SecureGo plus App

Im Namen eines Volksbank-Teams werden Phishing-SMS und -Mails versendet, in denen Betrüger behaupten, die Legitimation für die Nutzung der VR SecureGo plus App liefe bald ab. Um eine Sperrung abzuwenden, sollen die Bankkunden sich mit Ihren OnlineBanking-Daten auf einer Seite einloggen, die in der Nachricht verlinkt ist. Bei der verlinkten Seite handelt es sich um eine Phishing-Seite.

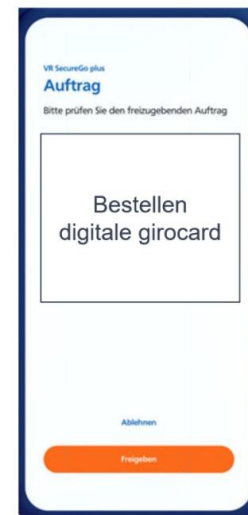
Digitale girocard

Beispielhafte Fallkonstellation:

SMISHING :

- SMS-Text:

<Volksbank>
Ihre SecureGo plus Synchronisierung endet am 23.03.2023. Bitte verlängern Sie ihre Legitimation unter <https://voba-securego-online.com/de/vo/index4ehp>











Passiv

Aktuelle Betrugsmaschen bei Zahlungssystemen

Fake-Shops

Angebote werden deutlich billiger präsentiert.
Überlegen Sie immer, ob das Produktangebot echt sein kann.

 <p>Michael Kors - MK Henkeltasc... 275,00 € Michael Kors - ... Kostenloser Ve... Von Google</p>	 <p>Michael Kors - Damen... 275,00 € Breuninger.com Kostenloser Ve... Von Shoparade</p>	 <p>Michael Kors - Tote - Jet Set... 163,70 € fashionette.de Kostenloser Ve... ★★★★★ (250) Von Adference...</p>	 <p>Michael Kors - Damen Shoppe... 295,00 € Breuninger.com Kostenloser Ve... Von Shoparade</p>	 <p>Michael Kors - Jet Set - Damen... 136,10 € Brandfield.de Kostenloser Ve... Von Producthero</p>	 <p>Michael Kors - Lillie Lg Chain... 449,99 € Peek & Cloppe... Kostenloser Ve... ★★★★★ (585) Von Producthero</p>	 <p>SALE MICHAEL Michael Kors - Tote Bag... 118,00 € 196-€ THE OUTNET +10,00 € Vers... Von Google</p>	 <p>Michael Kors - Tote - Voyager... 191,80 € fashionette.de Kostenloser Ve... ★★★★★ (550) Von Google</p>
---	---	---	--	---	---	---	---

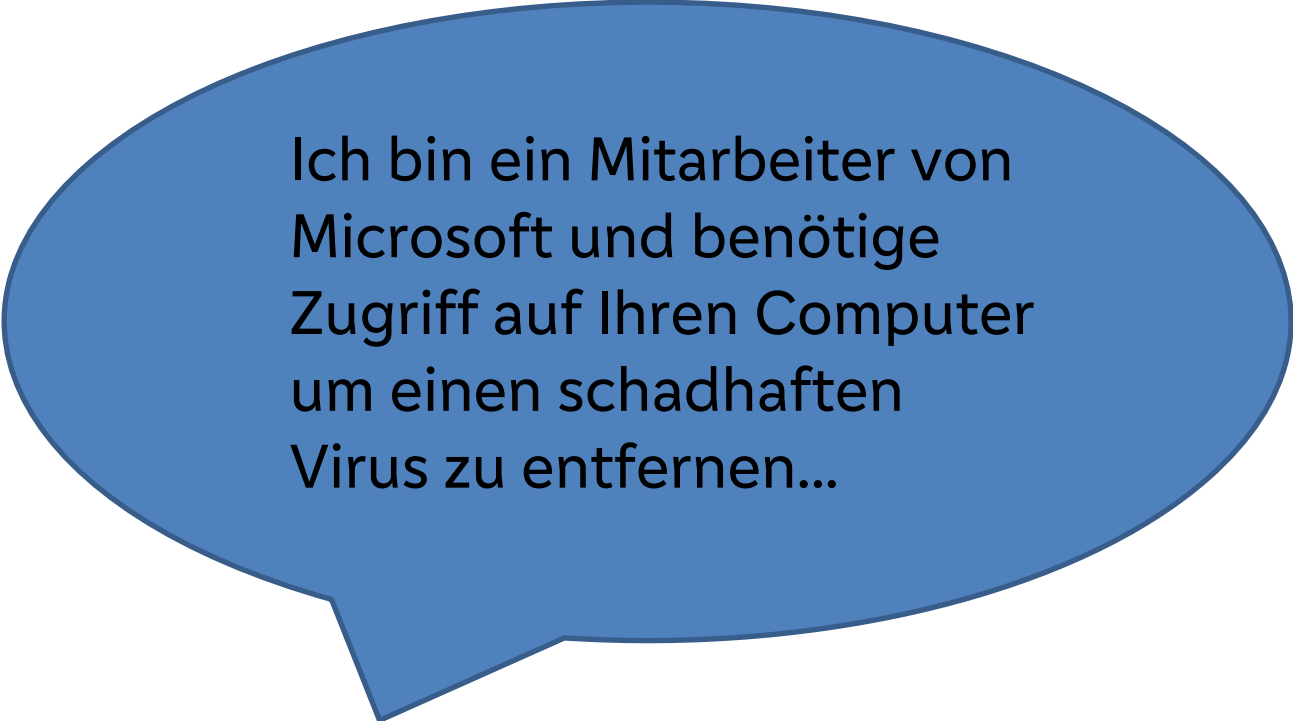
Aktuelle Betrugsmaschen bei Zahlungssystemen

Änderung der Bankverbindung

In Zeiten des elektronischen Zahlungsverkehrs werden Rechnungen in vielen Geschäftsbereichen nur noch elektronisch versandt. Diesen Umstand machen sich nun auch Kriminelle zu nutzen, indem sie böswillig auf den Nachrichtenaustausch zwischen Verkäufer/Dienstleister und Kunde einwirken. Die Täter nutzen hierzu verschiedene Methoden, um sich in die Kommunikation einzuschalten. Eines haben alle Vorgehensweisen jedoch gemeinsam: Die Mitteilung an den Kunden, dass sich die Bankverbindung des Rechnungsstellers angeblich geändert habe. Ist dieses Täuschungsmanöver beim Kunden erfolgreich, überweist dieser den tatsächlich offenen Rechnungsbetrag auf das Konto der Betrüger.

Aktuelle Betrugsmaschen bei Zahlungssystemen

Microsoft-Wartung mittels Fernwartung



Ich bin ein Mitarbeiter von
Microsoft und benötige
Zugriff auf Ihren Computer
um einen schadhaften
Virus zu entfernen...

Aktuelle Betrugsmaschen bei Zahlungssystemen

Geschäftsangebot, Gewinnversprechen, Erbzahlung,
Nigeria-Connection, Love-Scamming



Geschäftsangebot

Mr. Alan Austin An: Recipients

Blindkopie: ezy

Bitte Antwort an alan.austin047

Hallo,

Ich bin Alan Austin und arbeite derzeit bei der Credit Suisse Bank London. Ich habe Ihren Kontakt während meiner privaten Suche gesehen und bin fest davon überzeugt, dass Sie sehr ehrlich, engagiert und in der Lage sind, bei diesem Geschäftsvorhaben mitzuwirken.

Ich bin ein Kontobeamter des verstorbenen Dr. Manzoor Hassan, der mit seiner ganzen Familie in Sri Lanka bei Osterbombenanschlägen in seinem untergebrachten Luxushotel gestorben ist. Auf dieser Grundlage möchte ich Sie kontaktieren, damit Sie meinem verstorbenen Kunden als Nutznießer zur Seite stehen. Gelder in unserer Obhut werden freigegeben und an Sie als Begünstigten des Verstorbenen ausgezahlt.

Es ist wichtig, dass Sie mir mit Ihrem vollständigen Namen und Ihrer vollständigen Adresse antworten, einschließlich Ihrer direkten Telefonnummer, damit ich Ihnen alle Einzelheiten zu dieser Transaktion und weitere Informationen über meinen verstorbenen Kunden, der einen großen Geldbetrag in unserer Bank hinterlassen hat, mitteilen kann. Ich werde Ihnen alle erforderlichen Informationen, Unterlagen und Nachweise zur Verfügung stellen, um die Forderung der verschiedenen betroffenen Ämter nach einer reibungslosen Überweisung des Betrags auf eines Ihrer Konten als wahrer Begünstigter rechtmäßig zu belegen.

Dein,
Mr. Alan Austin

Aktuelle Betrugsmaschen bei Zahlungssystemen

Geschäftsangebot, Gewinnversprechen, Erbzahlung,
Nigeria-Connection, Love-Scamming

Beispiele

- Betrug mit vorgetäuschter Liebe
- Betrug mit falscher Identität (Soldat)
- Betrug mit Wohnungsangeboten
- Betrug mit dem Traumjob
- Betrug mit gefälschten Schecks
- Betrug mit falschen Geldversprechen



Aktuelle Betrugsmaschen bei Zahlungssystemen

Shops in Deutschland – IBAN beginnt nicht mit DE

Malta	31 an	5 - 13	MT84 MALT 0110 0001 2345 MTLC AST0 01S
Litauen	20 an	5 - 9	LT12 1000 0111 0100 1000
Island	26 an	5 - 8	IS14 0159 2600 7654 5510 7303 39



Ihre Fragen zu „Aktuelle Betrugsmaschen bei Zahlungssystemen“

Vielen Dank für Ihre Aufmerksamkeit

Volksbank Plochingen eG
Torsten Schwarz
Prokurist und Leiter Marktfolge Passiv
Am Fischbrunnen 8
73207 Plochingen
07153 706-271
torsten.schwarz@volksbank-plochingen.de

