Betrügereien 2020-2025

In den vergangenen Jahren waren es vor allem Erpresserviren, bei denen komplette Systeme verschlüsselt wurden und nur gegen immense Lösegeldzahlungen wieder freigeschaltet werden konnten. - **70 Kommunen 2023 in NRW durch Cyberangriff lahmgelegt** – Des weiteren treten seit ca. 2020 vermehrt Betrügereien auf, bei denen insbesondere ältere Menschen mittels Druckaufbau zu einem Ereignis z.B. aus dem familiären Umfeld unter Hinzuziehung von „Polizei, Rechtsanwalt, Ge-richt“ usw. um ihre Ersparnisse gebracht werden.

Neues vom Enkeltrick

- **Nachdem das Handy ja „heruntergefallen“ ist und dabei kaputt ging, hier eine neue Variante.**
- „Hallo, Oma hast du Fotos von mir? Ich habe nämlich mit dem kaputten Handy alle verloren“.
- **Es ist davon auszugehen, dass die Betrüger die Fotos für weitere kriminelle Zwecke verwenden wollen. Wieviel vertrauter kann man anschließend mit einem netten Foto „von sich“ die Oma um einen kleinen finanzielle Gefallen bitten.**
- **Also auf keinen Fall Fotos!!** WhatsApp könnte damit sehr familiär wirken

Polizeihauptwache – Kommissar Braun

In den letzten Jahren haben Ganoven immer wieder versucht über einem Schockanruf bei älteren Menschen an deren Erspartes zu gelangen. Hier ein einfacher Trick um derartige Anrufe ins Nirwana laufen zu lassen

Polizeihauptwache Kommissar Braun: (verlogener Gauner)

„Ihr Sohn hat heute einen schweren Unfall mit Personenschaden verursacht und ist deshalb vorläufig festgenommen worden. Gegen Vorlage einer Kaution von 5000 € kann er allerdings bis zur Hauptverhandlung auf freien Fuß gesetzt werden.“

Telefon-Betrüger: Rentnerin sagt falschem Polizisten die Meinung (t-online.de)

Ihre Gegenfragen:

Stop! Welcher? Ich habe nämlich **zwei** Söhne**. Den Anton und den Erich (Sie lügen jetzt ebenso) oder:**

Sie haben sicherlich den Unfall aufgenommen? „Ja“. Dann nennen Sie mir noch schnell sein Geburtsdatum!

Im Zweifel legen Sie den Hörer sofort auf und rufen die Polizei direkt neu an

Wie revanchiere ich mich für einen Schockanruf (ein Rollenspiel!)

- **Ein Schockanruf erreicht mich:**
- **„Ihr Enkel hat einen schweren Unfall mit Todesfolge verursacht!“** Nun mein Part als Schauspieler – ich „schauspielere“ nämlich wirklich gut!!! „Das ist ja sehr schlimm. Mein(e) Frau (Mann) darf davon um Gottes Willen nichts erfahren, sie (er) ist nämlich sehr herzkrank. Sie sind bei mir allerdings auf meinen Nebenanschluss gelandet. Für nähere Angaben zum Unfallhergang rufen Sie mich deshalb bitte umgehend unter meiner Hauptnummer an, da bekommt mein(e) Frau (Mann) wenigstens davon momentan nichts mit. Bitte rufen Sie mich unter der nachfolgenden Nummer an:
- **Diese ist: 08141 6120.“**
- **::**
- Hier meldet sich allerdings: **Polizeiinspektion Fürstenfeldbruck**
- **Und das ist mein „Gegenschock!“ Gelungen?**

Trickbetrüger ruft als Bank-Mitarbeiter an

- Ein Unbekannter gibt sich als Mitarbeiter Ihrer Bank aus.“
- ***Ich habe schlechte Nachrichten, Ihr Online-konto wurde gehackt! Wir müssen umgehend Ihre Daten prüfen. Geben Sie mir Ihre IBAN-Nr. an und aktivieren Sie Ihr mobiles TAN“***
- **(Puchheim Schaden 250000 €)**
- **Ihre Bank ruft Sie niemals an, nur auflegen.**

Polizei warnt vor neuen Whatsapp-Betrugsmasche

Der Anrufer gibt sich als **Mitarbeiter eines Bank-Sicherheitsservices** aus.

Er behauptet der Bank seien Unregelmäßigkeiten aufgefallen. Die Frau habe ihre letzte Abhebung an einem **manipulierten Kartenterminal** getätigt, wodurch Betrüger an die persönlichen Daten der Frau gelangt seien.

Denken Sie daran: Ihre Bank ruft Sie niemals an – Also sofort auflegen

Geldforderungen von Behörden: nur Papierform zulässig und vorgeschrieben

In der Regel verwenden Telefonbetrüger den Enkeltrick. Andere geben sich mal als Krankenkasse, Microsoft-Mitarbeiter, als Notar, Polizeibeamte, Rechtsanwalt, Finanzamt, Zoll, Bankangestellter, Europol, Deutsche Botschaft oder sogar als Mitarbeiter des Amtsgericht Frankfurt aus. Mit diesem Trick wollte selbst eine 14-Jährige per Telefonbetrug am 17.05.24 225.000 Euro von einer Seniorin ergaunern. Nur die war schlauer

Allen „Behörden“ gemein, ist nur die Betrugsabsicht.

Also auflegen

Amtsgericht München warnt und gibt Hinweise zur Prävention 12.03.24


Amtsgericht München

Amtsgericht München

BESTÄTIGUNG DES GERICHT

RECHTSSACHE:

LADUNG

zur Vernehmung als Partei

Eingang
27.02.2024

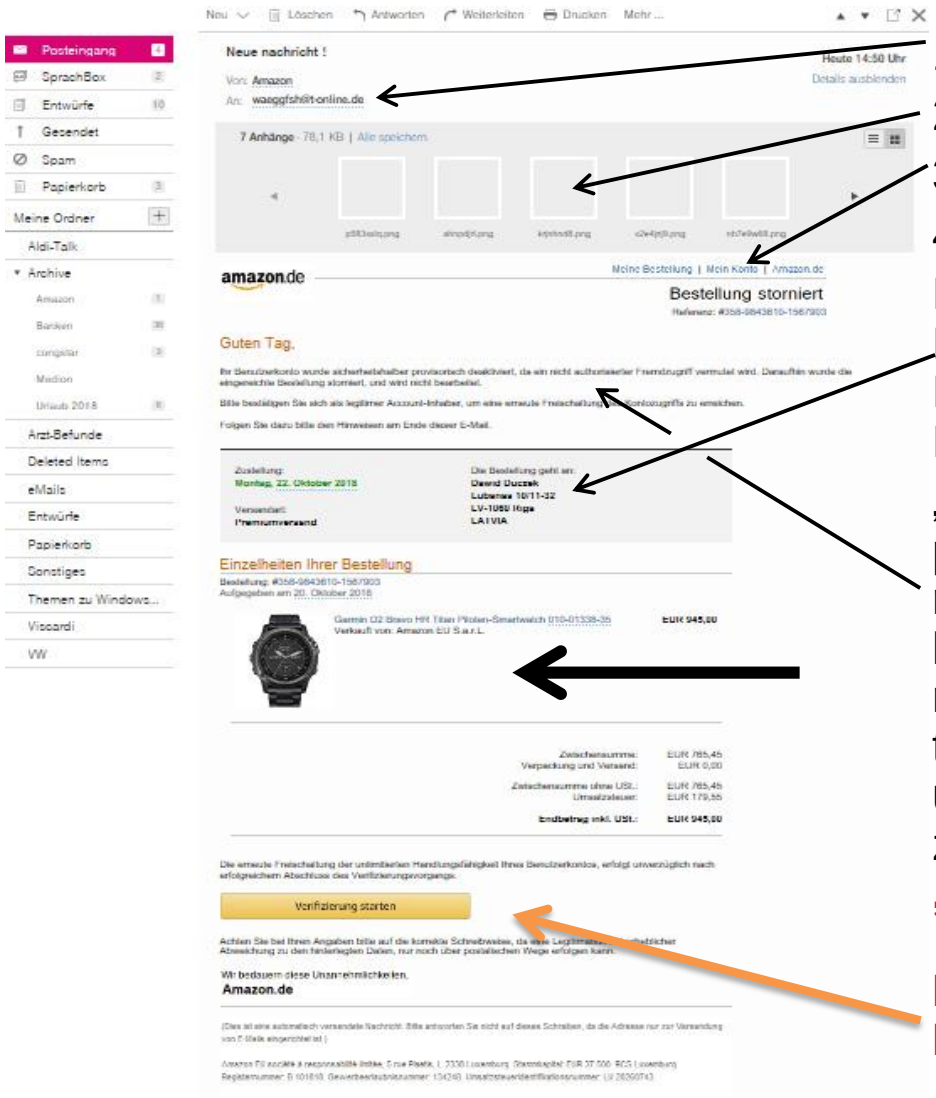
Angebliches Behördenschreiben des AG München ist eine **Fälschung per Briefpost**. Ein AG kann niemals durch eine Kanzlei vertreten werden. Auch Terminladungen eines Amtsgerichts können nicht durch andere Gerichte erfolgen. Hier soll wohl über eine Drohgebärde eine unberechtigte Zahlungsaufforderung getätigt werden.

Nur löschen

Nebulöse „Rechnungen“

- Scheuen Sie sich nicht eine Kopie der Rechnung an das Unternehmen, von dem diese Rechnung augenscheinlich stammt, zur Überprüfung zu senden. Dies sind speziell **AMAZON** und **Pay-pal.**
- **Ansonsten gleich in den Papierkorb**

Falsche Rechnung von „Amazon“



1) Adresse gekidnappt

2) 5+3 Pings **aktiv**

3) Meine Bestellung, mein Konto **inaktiv**

4) Besteller (nicht ich):

Dawid Duczek
Lubanas 10/11-32
LV-1060 Riga
LATVIA (Lettland)

„Ihr Benutzerkonto wurde sicherheitshalber provisorisch deaktiviert, da ein nicht autho-risierter Fremdzugriff vermutet wird. Darauf-hin wurde die eingereichte Bestellung stor-niert, und wird nicht bearbeitet. Bitte bestä-tigen Sie sich als legitimer Account-Inhaber, um eine erneute Freischaltung des Konto-zugriffs zu erreichen.“ **Vorsicht!! Text von „Amazon“ soll Sie in Sicherheit wiegen**

Hier ist die Falle: Niemals Ihre echten Daten eintragen

MELDUNG AN AMAZON

Sie haben eine eigentümliche Rechnung erhalten. Wenn Sie sich nicht im Klaren sind, so leiten Sie diese einfach weiter an Amazon. In wenigen Minuten erhalten Sie u.U. folgende Nachricht:

Guten Tag Herr[redacted],

vielen Dank für das freundliche Telefonat.

Wie besprochen stammt die E-Mail, die Sie erhalten haben, tatsächlich nicht von Amazon.de. Wir sind aber bereits dabei, der Angelegenheit genauer nachzugehen. Wenn möglich schicken Sie uns diese E-Mail als Anhang an: stop-spoofing@amazon.com . So bleiben alle Informationen der Kopfzeile erhalten, mit deren Hilfe wir die Herkunft der E-Mail besser nachverfolgen können. Löschen Sie danach die E-Mail. Wenn Sie die E-Mail nicht als Anhang verschicken können, leiten Sie sie bitte an stop-spoofing@amazon.com weiter. Geben Sie dazu die Information in der Kopfzeile an, wenn dies möglich ist.

Bitte beachten Sie, dass die E-Mail-Adresse **stop-spoofing@amazon.com** von unserer amerikanischen Website Amazon.com betreut wird und Sie daher eine Empfangsbestätigung auf Englisch erhalten werden. Wenn Sie die Mail weder als Anhang senden noch diese weiterleiten können, kann es sein, dass Ihr E-Mail-Provider das Weiterleiten einer bereits erkannten Phishing-Mail blockiert. In diesem Fall möchten wir Sie bitten, keine Links oder Anhänge zu öffnen und die E-Mail einfach zu löschen.

Sie erhalten wichtige Informationen des Kundenservice wie Aktualisierungen der Kontorichtlinien oder Produktrückrufe auch über das Message Center. Sie können das Message Center auch direkt über folgenden Link aufrufen:

https://www.amazon.de/gp/message

Verbraucherschutz warnt: So einfach bezahlen Betrüger mit Ihrem Paypal-Konto

Eine fiese Betrugsmasche über Paypal erlaubt es, einfach Abbuchungen auf Ihrem Namen durchzuführen. Es gibt kaum Möglichkeiten, sich davor zu schützen. Paypal ist eine beliebte Methode, um Online-Zahlungen zu tätigen. Aktuell vermehren sich die Berichte über eine Betrugsmasche, vor der man sich kaum schützen kann.

Verbraucherschützer warnen vor sogenannten **Gastkonten** auf Paypal, die es Dritten erschreckend einfach erlaubt, Abbuchungen im Namen des Kontoinhabers durchzuführen. Mit gefülltem Warenkorb geht er im Online-Shop zur Kasse. Hier wählt er als Zahlungsart Paypal, meldet sich aber nicht mit seinem Konto an, sondern klickt auf **Gast**; er zahlt also mit einem Gastkonto. Er bestellt das Produkt und gibt **seine eigene Adresse**, aber die **IBAN von jemand anderem an**, der vielleicht ein Paypal-Konto besitzt (die IBAN könnte zum Beispiel gestohlen sein, oder man hat sie vorher durch Phishing weitergegeben). Der Kauf geht durch, Paypal prüft die Daten nicht ausreichend nach und der echte Kontobesitzer bekommt die Abbuchung. Als andere Zahlungsart wählen Sie lieber Klarna. **Klarna** ist ein schwedischer Zahlungsanbieter mit Hauptsitz in Stockholm, der diese Zahlungsmöglichkeiten nicht anbietet und damit den o.a. Betrug ausschließt.

Wie wehren Sie sich gegen die aktuelle Paypal-Betrugsmasche

Eine Paypal-Bezahloption, die sich "**Zahlen ohne Paypal-Konto**" nennt und auch als "**Gast-Konto**" oder "**Gastzahlung**" bekannt ist, steht in der Kritik. Damit können Käufer im Lastschrift-Verfahren zahlen, ohne dass ein Paypal-Konto angelegt wird. Dafür ist eine IBAN anzugeben. Auf die Frage, ob eine Prüfung stattfindet, ob die IBAN der bestellenden Person tatsächlich gehört, antwortete Paypal eher ausweichend.

Betroffene können sich gegen die unberechtigten Zahlungen jedoch wehren. **Zunächst müssen sie dazu der Forderung des Unternehmens widersprechen**, da die Abbuchung unerlaubt stattfand, erklärt die Verbraucherzentrale NRW. **Lassen Sie den Betrag von der Bank zurückbuchen**, wofür ihnen normalerweise acht Wochen Zeit nach Buchungsdatum bleiben – bei unberechtigten Buchungen jedoch sogar 13 Monate. Wichtig ist auch eine **Anzeige bei der Polizei wegen Datenmissbrauch**.

Inkassoforderungen lassen sich durch Vorlage der Anzeige bestreiten, erörtert die Verbraucherzentrale.

PayPal-Betrug: Vorsicht bei Geld von Fremden

So funktioniert die Betrugsmasche, die zurzeit ihre Runden macht. So erhalten vermehrt PayPal-Nutzer eine Geldsumme von einem unbekannten Account. Kurze Zeit später folgt jedoch die folgende Nachricht: „Entschuldigung, ich habe mich bei der E-Mail-Adresse vertan. Könnten Sie das Geld über die **Option ‚Freunde und Familie'** zurücksenden, aber auf ein anderes Konto?“ **Nein!**

<u>Falle</u>: Ggf. behalten Sie einfach das Geld und warten ab, ob der Betrüger Anzeige erstattet.

17.05.24

Neue DHL-Betrugsmasche mit Paketsendungen

ZAHLUNG VON EINFUHRZÖLLEN/STEUERN ERFORDERLICH

Sehr geehrte/r geschätzte/r Kunde/in,

Ihre Sendung ist im Land eingetroffen und hat den Zoll passiert. Es steht jedoch eine offene Einfuhrzoll-/Steuerzahlung aus, die beglichen werden muss.

Bitte beachten Sie, dass Ihre Sendung erst nach Klärung dieser Angelegenheit für die Zustellung freigegeben wird.

Wir empfehlen Ihnen, den Fortschritt Ihrer Sendung online weiter zu verfolgen.

Meine Sendung freigeben

Erst bei „Zahlung“ der Zollgebühren erfolge Auslieferung.
Nicht beachten – alles Fake

Im Zuge der amerikanischen „Zollorgie“ versuchen Betrüger es wieder mit der DHL-Tour. Klicken Sie deshalb niemals auf Links aus solchen Nachrichten wie nebenstehend und prüfen Sie den Sendungsstatus direkt über die offizielle DHL-App oder Website. Achten Sie auf Anomalien in der persönlichen Anrede, Sendungsnummer und offizielle Absenderadresse in der Sendung. Waren, die Sie nicht bestellt haben – **Annahme verweigern**, ebenso Waren an den Nachbarn, insbesondere **Nachname-Sendungen**. Die Täter professionalisieren ihre Methoden kontinuierlich. Mit KI erstellen sie fehlerfreie Nachrichten. QR-Codes werden vermehrt eingesetzt. Gefährlich sind Links oder Anhänge, die Schadsoftware wie Trojaner oder Ransomware installieren. Niemals unerwartete Anhänge öffnen und verdächtige Links meiden.

Bankmitarbeiterin getäuscht: Betrüger ergaunern sechsstellige Summe

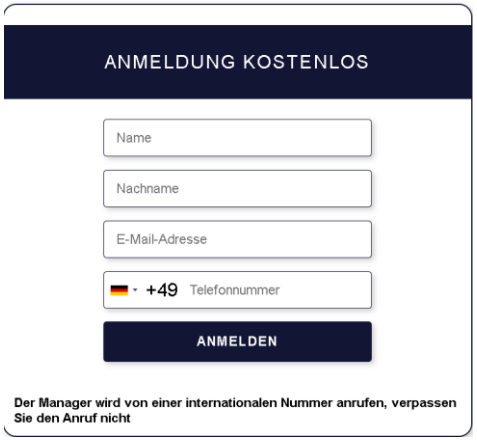
Ein Telefonbetrüger hat am Dienstag eine Bankmitarbeiterin getäuscht und damit erheblichen finanziellen Schaden angerichtet.

Nach Angaben der Polizei kontaktierte der unbekannte Anrufer am Vormittag die Bank und gab sich als Geschäftsführer (CEO-Fraud) eines örtlichen Unternehmens aus. Durch geschickte Gesprächsführung setzte er die Mitarbeiterin so stark unter Druck, dass sie mehrere Überweisungen anordnete. Einige der Überweisungen wurden ausgeführt, bevor der Betrug erkannt wurde. Zwar konnten mehrere Transaktionen rückgängig gemacht werden, dennoch entstand ein Schaden im unteren sechsstelligen Bereich. Die Kriminalpolizei hat die Ermittlungen aufgenommen und warnt vor dieser Betrugsmasche, bekannt als „**CEO-Fraud**“.Dabei geben sich Betrüger als Führungskräfte von Unternehmen aus und wenden sich gezielt an **Mitarbeiter, die Überweisungen tätigen dürfen**. Diese werden unter Druck gesetzt, größere Summen ins Ausland zu überweisen. Die finanziellen Schäden können bis in die Millionenhöhe reichen. Die Polizei rät Unternehmen, Schutzmaßnahmen zu ergreifen: Mitarbeiter sollten klare Vorgehensweisen für finanzielle Transaktionen kennen und bei ungewöhnlichen Anweisungen stets eine Rückversicherung einholen.

- 24.02.2025

„Deutsche Bank“ verspricht 10000€/Mon.

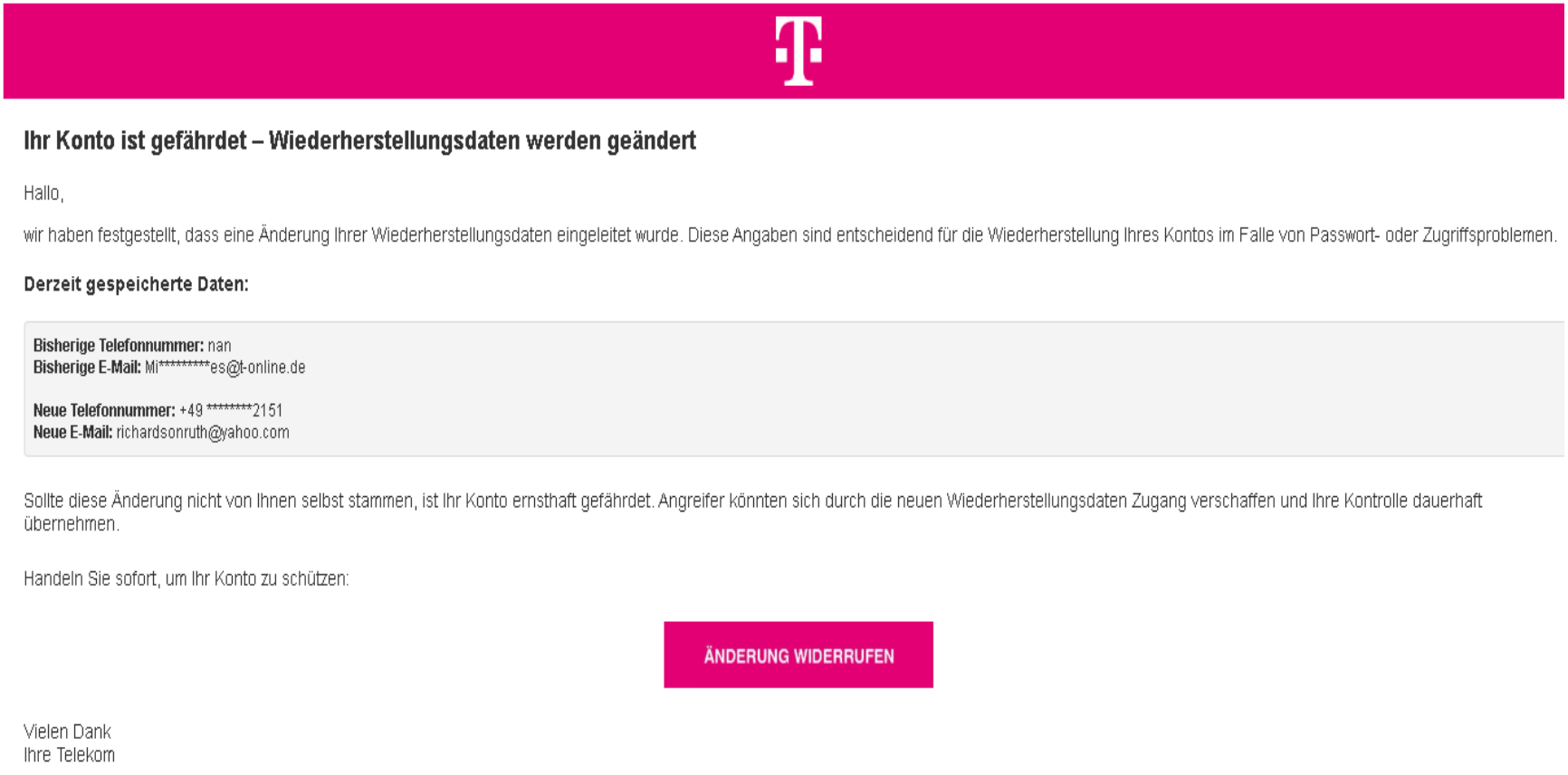
Dies ist eine **Betrugs-eMail** der „Deutschen Bank“. Jede seriöse Bank bzw. Firma führt am Ende Ihrer Anzeige jeweils ein IMPRESSUM. Darin enthalten sind alle gängigen Angaben wie Ort, Strasse, Haus-Nr sowie Telefon/Fax und eMail-Adresse. Geht hier nicht! Egal auf welche Eintragungen am Ende der Anzeige Sie klicken, die Ganoven wollen Sie zwingen, Ihre Telefon-Nr, o. eMail-Adresse anzugeben. Sie werden von einer „internationalen Nr“ zurückgerufen. Gewinnversprechen unmöglich!! Sie können den HyperLink zur Demo jederzeit öffnen. **Aber bitte keine Angaben in die Anmeldung eintragen!**



https://cipiqoo6.pro/FU1JFhk9jLqXUYbpPOS3rsHqR5NH5SVOLHPR2pTRqGIpYNoD6RtEroEDwACWOw6lGS8xvdjw2J3yTfdufoG2Pf3QHpeW20wQ7FdTPUNaLOUUbcdcbyvh8fg99OX43ffpQYT-u9Wx1wTldS5Ihpy1Qw/?googleIdTh={googleIdTh}&lf_utm_source={lf_utm_source}&**lf_utm_medium**={lf_utm_medium}&lf_utm_campaign={lf_utm_campaign}&lf_utm_content={lf_utm_content}&lf_utm_term={lf_utm_term}&lf_subid1={lf_subid1}&lf_subid2={lf_subid2}&lf_subid3={lf_subid3}&lf_subid4={lf_subid4}&lf_subid5={lf_subid5}&dlp=https%3A%2F%2Fpersimmonbulldog.pro&stream_uuid=d6b632c0-bbcb-4d18-ba16-6dc09f8b725d&utm_term=100002&blp=1&t_id={t_id}&utm_source=luckypush&lang={lang}&turl={turl}&polid=2&external_id=&redir=1&subid1=1ut7irnnuomh

- **29.09.2025**

Fake! Konto ist gefährdet? Nein! Wiederherstellungsdaten wurden geändert.



Ihr Konto ist gefährdet – Wiederherstellungsdaten werden geändert

Hallo,

wir haben festgestellt, dass eine Änderung Ihrer Wiederherstellungsdaten eingeleitet wurde. Diese Angaben sind entscheidend für die Wiederherstellung Ihres Kontos im Falle von Passwort- oder Zugriffsproblemen.

Derzeit gespeicherte Daten:

Bisherige Telefonnummer: nan
Bisherige E-Mail: Mi*********es@t-online.de

Neue Telefonnummer: +49 ********2151
Neue E-Mail: richardsonruth@yahoo.com

Sollte diese Änderung nicht von Ihnen selbst stammen, ist Ihr Konto ernsthaft gefährdet. Angreifer könnten sich durch die neuen Wiederherstellungsdaten Zugang verschaffen und Ihre Kontrolle dauerhaft übernehmen.

Handeln Sie sofort, um Ihr Konto zu schützen:

ÄNDERUNG WIDERRUFEN

Vielen Dank
Ihre Telekom

Mein Konto ist nicht gefährdet. Ich habe vor ca 15 Jahren meine eMail-Adresse geändert. Diese alte Adresse taucht nun fragmentiert wieder auf, mit dem Hinweis das Konto sei ernsthaft gefährdet und Wiederherstellungsdaten seien geändert worden.

Telekom-Mail Sicherheitsteam: Diese Aufforderung sollten Sie ernst nehmen

Schild mit Telekom-Logo: Nach einem Datenklau sollten Sie Ihr Passwort ändern.

[redacted]

Ticket-Nummer: [redacted],
Ihre Daten wurden gestohlen
und sind im Internet einsehbar

Posteingang

Telekom Sicherheitsteam 02:32
an mich, [redacted]

| Kundennummer: [redacted]
| Anschlussinhaber: [redacted]

Sehr geehrter Herr [redacted]

im Rahmen der Missbrauchsprävention erhalten unsere Sicherheitsexperten Hinweise auf illegale Veröffentlichungen von Kundendaten. Bei den Recherchen ist aufgefallen, dass Ihre Login-Daten missbräuchlich entwendet wurden und im Internet angeboten werden.

Es handelt sich dabei um folgende Daten für Ihren Hauptnutzer mit der Zugangsnummer [redacted]

Diese Daten können genutzt werden, um zum Beispiel über unsere Portale kostenpflichtige Produkte zu Ihren Lasten zu erwerben oder Einstellungen in Ihrem Kunden- und/oder Telefoniecenter vorzunehmen, die erhebliche Kosten für Sie zur Folge haben.

Zu Ihrer eigenen Sicherheit werden Sie beim Login ins Kundencenter unter https://kundencenter.telekom.de umgeleitet, um sich ein neues Passwort zu vergeben. Dies ist besonders wichtig, da auch Einstellungen für Ihre Telefonie (z.B.

10 Milliarden Passwörter geleakt – So prüfen Sie, ob Ihre Daten betroffen sind

Passwort gehackt? Mit diesem Check finden Sie es heraus:

Im Juli diesen Jahres sind durch den wohl größten Leak aller Zeiten rund **10 Milliarden Klartextpasswörter** ins Netz gelangt. Noch immer gibt es Betroffene, die nicht wissen, ob ihr Passwort kompromittiert wurde. Wir erklären Ihnen, wie Sie überprüfen, ob Ihr Account betroffen ist und was jetzt zu tun ist. Überprüfen Sie Ihre Konten regelmäßig auf ungewöhnliche Aktivitäten. Das können zum Beispiel Anmeldungen von ungewöhnlichen Orten oder Geräten sein, die Sie nicht erkennen. Erhalten Sie E-Mails von Online-Diensten über Änderungen an Ihren Kontoeinstellungen, die Sie nicht selbst vorgenommen haben? Das könnte darauf hinweisen, dass jemand unbefugt auf Ihr Konto zugegriffen hat. Wenn Sie sich plötzlich nicht mehr in Ihre Konten einloggen können, obwohl Sie sicher sind, dass Sie die richtigen Anmeldeinformationen verwenden, sollten Sie alarmiert sein. Dies könnte darauf hindeuten, dass jemand Ihr Passwort geändert hat.

Auf der Seite des Hasso-Plattner-Instituts finden Sie den **Identity Leak Checker**. Hier können Sie Ihre E-Mail-Adresse angeben und so prüfen, ob diese oder andere sensible Daten gehackt wurden und im Netz verfügbar sind.

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	–	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–	–

Warnung Ihrer Sparkasse

Vorsicht vor „Quishing“, einer neuen Betrugsmasche

Neben eMails und Anrufen sind ***neuerdings*** **Briefe** - angeblich im Namen des Deutschen Sparkassen- und Giroverbands - aufgetaucht. Die Sparkasse warnt eindringlich.

Sparkasse warnt vor betrügerischen Briefen

In den Briefen wird die Aktualisierung persönlicher Daten gefordert. Dafür ist im Schreiben ein **QR-Code** angegeben. Wird der Code gescannt, wird man automatisch auf eine betrügerische Webseite umgeleitet – auch Phishing-Seite genannt. An dieser Stelle werden neben persönlichen Daten auch die Zugangs-Daten für das Online-Banking sowie die Nummer der Sparkassen-Card oder Kreditkarte abgefragt.

Die Sparkasse warnt nachdrücklich: „Bitte geben Sie niemals Daten auf den Phishing-Seiten ein.

Nach Kenntnis Ihrer Zugangsdaten wird das Passwort geändert und Sie haben auch als Kontoinhaber hierauf keinen Zugriff mehr, so dass in aller Ruhe Ihr Konto geplündert werden kann

So erkennen Sie den falschen Sparkassen-Brief

Mit fadenscheiniger Begründung für die Daten-Abgabe wird von den Betrügern auf eine „EU-Vorschrift zur Verhinderung von Geldwäsche und den Know Your Customer (KY C) Richtlinien“ verwiesen. Außerdem heißt es, dass das Online-Banking eingeschränkt wird, sollte man den Brief missachten. **Alles nur Fake**.

Was kann man tun, wenn man Daten ein- oder angegeben hat?

Wenn Sie bereits auf die Betrugsmasche hereingefallen sind, wenden Sie sich **auf direktem und offiziellem Weg an die Sparkasse**. Vor Ort können die Mitarbeiter den Zugang zum Online-Banking und die Kredit- und Sparkassenkarte sperren. Dadurch wird finanzieller Schaden verringert oder sogar verhindert.

Häufig sind Betrugsmaschen kompliziert. Bei dieser neuen Methode ist das jedoch anders: Sie ist sehr einfach und bringt den Tätern viel Geld

Ihre eMail liefert Ganoven Ihre Anrede frei Haus

Viele Internet-User verwenden in ihrer eMail-Adresse **ihren eigenen Vornamen und Nachnamen**.

Sofern Sie Schreiben mit betrügerischem Hintergrund erhalten, können die Ganoven diese hier in der Anrede gleich mitverwenden und erwecken damit einen persönlichen Eindruck.

Wenn aus eMail-Adressen diese Informationen nicht abgeleitet werden können, erkennen Sie sofort die **Betrugsabsicht**, denn diese Anschreiben mit einer unpersönlichen Anrede sehen immer so aus:

Sehr verehrter Kunde …

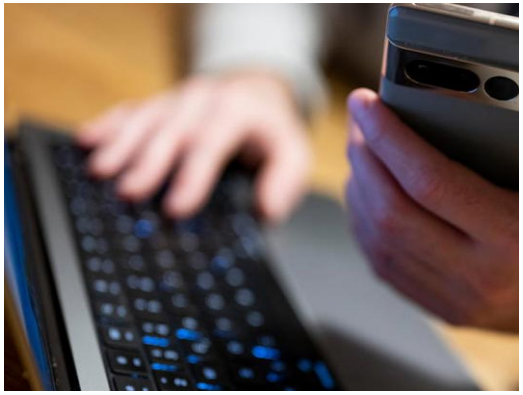
Ihre Dummheit, wenn Sie darauf hereinfallen. In aller Regel werden hier u.U. nicht vorhandene Schulden angemahnt oder „Bankkontodaten berichtigt“. Wenn Sie die eMail öffnen und hier auf Abfragen antworten, brauchen Sie sich nicht zu wundern, wenn Ihr Konto unbefugterweise um erhebliche Geldbeträge erleichtert wird.

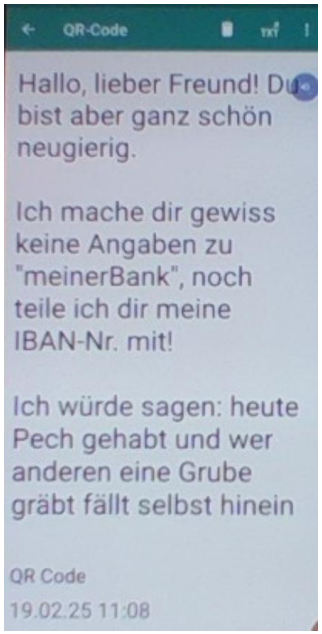
Deshalb Neugier unterdrücken und eMail nur löschen

Per Post zum Betrugsversuch **niemals** QR-Code abscannen

Gefälschte Strafzettel: Polizei warnt vor falschen QR-Codes

16.09.24





Gefährlich wird es auch für Falschparker: Polizei/Ordnungsamt setzen immer häufiger QR-Codes auf Strafzetteln ein, um **Bürgern die Bezahlung des Bußgeldes zu erleichtern?**

Dies ist kein Ersatz für einen Bußgeldbescheid!

Betrüger haben dies sofort in der Vergangenheit ausgenutzt und z.B. **gefälschte Strafzettel mit „QR-Codes“** an der Windschutzscheibe des Autos angebracht. **Vorsicht**: Gefälschte **QR-Codes auch an Ladesäulen,** oder postalisch versandte Schreiben **der „Commerzbank“ mit QR-Code! Sie werden damit nur betrogen.**

In einen QR-Code passen 7089 Zahlen und 4296 Buchstaben: Und damit lassen sich in Kombination viele Betrügereien bewerkstelligen.

Deshalb, Vorsicht beim Abscannen des Codes der „Commerzbank“! Nie darauf reagieren!

Oder telefonische Rückfrage bei Ihrer Bank

Beileigender QR-Code ist Test, nur ein Muster

Bußgeldbescheid per QR-Code

Ein Bußgeldbescheid, der nur über einen QR-Code auf einer Postkarte ohne Adressaten zugestellt wird, wäre in Deutschland **rechtlich unzulässig**. Hier sind die wesentlichen Gründe:

Formvorschriften des Bußgeldbescheids:

Ein Bußgeldbescheid muss nach § 66 des **Ordnungswidrigkeitengesetzes (OWiG)** zwingend bestimmte Angaben enthalten, darunter:

Den **Betroffenen namentlich benennen**
Die **Tatbezeichnung**
Die **Rechtsgrundlage**
Die **Beweismittel**
Die **Rechtsbehelfsbelehrung**

Ein QR-Code alleine ersetzt diese Angaben nicht und erfüllt die gesetzlichen Anforderungen nicht.

Zustellungsvorschriften: Ein Bußgeldbescheid muss in Deutschland in der Regel **per Post mit Zustellungsnachweis** erfolgen (§ 51 OWiG i.V.m. §§ 3, 5 Verwaltungszustellungsgesetz).

Eine **Postkarte ohne Adressaten** wäre **kein sicherer Zustellweg** und könnte leicht verloren gehen oder von Unbefugten eingesehen werden, was **datenschutzrechtlich problematisch** wäre.

Datenschutz & Persönlichkeitsrechte:

Ein Bußgeldbescheid enthält **personenbezogene Daten** und unterliegt dem **Datenschutzrecht (DSGVO, BDSG)**.

Eine offene Postkarte ohne sicheren Briefumschlag wäre ein klarer **Verstoß gegen den Datenschutz**, da Dritte Zugang zu den Daten hätten.

Fazit

Ein Bußgeldbescheid nur per QR-Code auf einer Postkarte ohne Adressaten ist **nicht zulässig**. Sollte dir ein solcher Bescheid zugehen, kannst du **rechtliche Schritte einleiten**, insbesondere einen Einspruch einlegen und ggf. die Rechtswidrigkeit der Zustellung rügen.

Falsche QR-Codes auf Parkautomaten:

Auf Parkautomaten in Hannover wurden vor Kurzem gefälschte QR-Codes der Parkschein-App "EasyPark" entdeckt. Anscheinend sollten Bezahldaten von Nutzern entwendet werden. Die Polizei nahm vorübergehend drei Heranwachsende fest, die eine Rolle mit gefälschten QR-Code-Aufklebern bei sich trugen. Ihren Angaben zufolge hatten sie von „Mitarbeitern der Easy Park“ gegen Entlohnung für ihre Mithilfe zur „Berichtigung“ der „fehlerbehafteten QR-Codes“ durch Überkleben eine Entlohnung in Geld erhalten. Die Polizei Hannover stellte die gefälschten Rollen sicher. Anzeige gegen unbekannt wurde erstellt. Eine weitere Verfremdung durch Überkleben des ursprünglichen QR-Codes durch betrügerische neue Sticker konnte verhindert werden.

Vor neuer Betrugsmasche, bei der Täter über die originalen QR-Codes auf Automaten einen QR-Code klebten, der auf eine gefälschte EasyPark-Internetseite führte, wird gewarnt. Dort wurden die Nutzer laut Landeskriminalamt (LKA) aufgefordert, neben der Parkzeit ihre Kreditkartendaten einzugeben.

Vorsicht, Quishing! Virenscanner erkennen keine QR-Codes !!

So gehen die Cyberkriminellen vor In der neuen Variante des Quishings geht es angeblich um die regelmäßige Überprüfung der Identität eines Bankkunden aufgrund von EU-Vorschriften. Um dies so einfach wie möglich zu gestalten, soll man den auf dem Anschreiben abgebildeten QR-Code einscannen. Beim Online-Quishing wird in der Betreffzeile der E-Mails zum Beispiel auf ein Sicherheitsproblem hingewiesen, bei dem die Nutzer aktiv werden müssten. Das Ziel der Betrüger ist immer, dass die Nutzer den QR-Code auf ihrem Smartphone einscannen

Tipps, um nicht auf Quishing hereinzufallen

Prüfen Sie sorgfältig, ob es sich bei der Mail oder dem Brief um eine Fälschung handeln könnte. Kontaktieren Sie den vermeintlichen Absender über offizielle Kanäle. Meist ist die angegebene Telefonnummer nicht geschaltet. Bei einem Post-Brief sollte man sicherheitshalber den persönlichen Bankberater anrufen und den Sachverhalt offiziell abklären. Der Empfänger eines solchen eMail bzw. Brief sollte bei der Polizei Anzeige erstatten und dabei das eingescannte oder originale Täterschreiben vorlegen. Wer darauf hereingefallen ist, sollte unverzüglich sein Kreditinstitut informieren und den Zugang sperren lassen. Hierfür kann auch der Sperrnotruf genutzt werden. +49 116 11

Angriffe über Tricks mit QR-Codes

Die Angriffe kommen per E-Mail und umgehen viele üblichen Sicherheitsscans. Liest man die eMails dann auch noch mit aktivierter HTML-Darstellung, wird man leicht zum Opfer.

QR-Codes sind bei Verbrechern beliebt, weil sich darin Hyperlinks kodieren lassen, die Menschen nicht lesen können. Damit lassen sich sehr leicht falsche Hyperlinks unterjubeln. Wird der Code eingescannt, landet man auf einer vom Angreifer kontrollierten Webseite und wird so zum **Ernten Ihrer Zugangsdaten** genutzt.

Separate Dateien ergeben zusammen ein Bild

Eine verblüffend einfache Methode besteht darin, einen irreführenden **QR-Code in zwei (oder mehr) Teile zu teilen**. Diese Bilddateien werden beispielsweise einem Phishing-eMail angehängt. Sicherheitssysteme versuchen in der Regel, die Bilddateien einzeln auszuwerten, finden in den einzelnen QR-Schnipseln aber nichts Verwertbares und lassen die gefährliche Nachricht passieren. **Mittels HTML** können die Bilder allerdings am Endgerät des Nutzers so angeordnet werden, dass sie optisch **wie ein einzelnes Bild** wirken.

Werden **zwei QR-Codes in einander zu verschachtelt**, kann Ihr Smartphone entscheiden wenn es lesen will.

ASCII-Code QR

Bereits im Oktober hat Barracuda über gefinkelte QR-Codes berichtet, die gar nicht als Bilddatei daherkommen, sondern aus ASCII-Codes zusammengesetzt sind, da-mit lassen sich Textgebilde erstellen, die von Smartphones als QR-Code erkannt werden

Angreifer profitieren mit QR-Codes von einem speziellen Vorteil: Sie lassen sich in der Regel nicht mit demselben Endgerät auswerten, auf dem sie angezeigt werden und man muss so in aller Regel zum Smartphone greifen.

Deshalb sind außerhalb geschlossener Systeme **QR-Codes grundsätzlich verdächtig** und mit einer gehörigen Portion Argwohn zu begegnen.

Schadsoftware im Umlauf:

Kriminelle haben das Internet längst als Schauplatz für ihre Betrugsmaschen entdeckt.

Jetzt nutzen sie sogar die Tatsache, dass man sich auf vielen Webseiten **verifizieren** muss, um ihre Schadsoftware zu verbreiten. Eine ähnliche Masche gab es mit einem „**Sicher bezahlen**“-Button bei Kleinanzeigen.

Ein öffentliches Amt warnt mittlerweile vor der Gefahr durch die betrügerischen Captchas und gibt Hinweise, wie man sich schützt.

Bei „**verifizieren**“ Vorsicht geboten

Die Masche läuft folgendermaßen ab:

Bereits mit dem Setzen des Häkchens beim „**Ich bin kein Roboter**“-Captcha wird ein schädlicher Befehl in die Zwischenablage kopiert.

Im zweiten Banner sollen Nutzer dann per Tastenkombination ein Windows-Eingabefeld öffnen.

Eine weitere Tastenkombination soll den schädlichen Befehl aus der Zwischenablage in das Eingabefeld einfügen und ausführen.

Der Server des Angreifers lädt dann eine Schadsoftware herunter und installiert sie, um den PC zu übernehmen und erheblichen Schaden anzurichten.

Unbekannte Abbuchungen vom Konto:

Warnung vor Betrugsmasche

Gar nicht mal großen Summen wurden abgebucht. Das macht die Masche aus Sicht eines Users so perfide. Ein Ehepaar entdeckte rechtzeitig unbekannte Abbuchungen auf ihrem Konto. Und da hatte ein Betrüger schon regelmäßig unverfängliche Beträge von je 89,90 € abgebucht. Im heutigen Zeitalter des bargeldlosen Zahlungsverkehrs fällt so etwas so schnell einfach nicht mehr auf. Dies fiel eben diesem Geschädigten dann doch auf, nachdem er als Konsequenz ganz engmaschig die Bewegungen auf dem eigenen Konto verfolgt– **und das auch jedem anderen rät**. Sonst drohe schnell eine böse Überraschung. Dabei wurde entdeckt, dass eine unbekannte Adresse regelmäßig Geld vom Familienkonto abbuchte. Eine Summe, die man bei flüchtigem Blick über die Kontobewegungen auch mal übergehen kann– selbst wenn man regelmäßig den Kontostand und die jüngsten Buchungen kontrolliert. Aber nicht so bei der Kontokontrolle im Folgemonat. Da stachen die 89,90 € ins Auge, abgebucht als Basislastschrift der ***Firma Megatipp Emergency Call Services***. Gemeinsam mit einem Bankmitarbeiter wurde anhand der IBAN eine Bank auf Malta ermittelt. Besagte Summe von 89,90 € war dem Text auf dem Formular zufolge berechnet worden für eine Notfalll-Karte, als Telefonnummer war eine Verbindung mit der Ortsvorwahl vermerkt. Vermutlich muss der „regelmäßigen“ Abbuchung ein Telefonat vor Monaten vorausgegangen sein, bei dem das Opfer auf eine bestimmte Frage mit “Ja“ geantwortet hatte. Glücklicherweise bewegten sich die Abbuchungen noch im Zeitraum von acht Wochen und konnten so von der Bank noch zurückgebucht werden. Möglicherweise ist der Kontoinhaber mit der Rückbuchung der beiden Abbuchungen auch noch nicht ganz durch. Selbst wenn erneut abgebucht werden sollte und man dann der Empfehlung der Bank folgt, die Nummer zu sperren. In Internet-Foren ist die Rede davon, dass von „**Megatipp Emergency Call Services**“ möglicherweise noch Schriftverkehr wie etwa Mahnungen folgen könnte. Und dann muss unter Umständen der ungewollt untergejubelte Vertrag noch gekündigt werden, wozu sich manch einer auch schnell mal professionellen Beistand sichert– mit entsprechenden Kosten.

Zusammenstellung der Qishing-Maschen

Gefälschte Postbriefe: Als neue Masche verschicken Cyberkriminelle perfekt nachgemachte Postbriefe, die angeblich vom Bundesverband deutscher Banken oder von der Finanzgruppe deutscher Sparkassen stammen. Viele Kunden halten diese von der Deutschen Post verschick-ten Briefe für vertrauenswürdig und scannen den mitgeschickten QR-Code.

Gefälschte Strafzettel: Vor allem Falschparker bekommen hinter die Scheibenwischer geklemmte, täuschend echt aussehende Strafzettel. Für die Bezahlung soll man bloß den falschen QR-Codes einscannen und die dortigen Anweisungen befolgen.

Überklebte QR-Codes: Bei Parkautomaten und Elektro-Ladesäulen wurden echte QR-Codes mit gefälschten geschickt überklebt. Besonders perfide ist die Masche, bei der nach dem Ein-tippen der Bezahldaten eine Störung gemeldet wird. Erst im zweiten Anlauf gelangen die Opfer zur richtigen Webseite des Betreibers und vergessen den ersten Fehlversuch.

Manipulierte Rechnungen: In Papierdokumenten und vor allem in Speisekarten und Rechnungen können **Hacker** gefälschte QR-Codes verstecken. Das Bezahlen soll nur über diese QR-Codes mög lich sein. Nicht nur im Urlaub werden dabei stark überhöhte Kosten von den Bankkonten der Betroffenen abgezogen.

Gefälschte SMS und WhatsApp-Nachrichten: Immer häufiger verschicken Betrüger gefälschte QR-Codes per SMS oder WhatsApp. Diese Mitteilungen stammen angeblich von bekannten Unter nehmen oder von öffentlichen Stellen. Dort wird behauptet, dass die Empfänger noch ihre Schulden bezahlen und dazu den QR-Code nutzen müssten.

Gefälschte E-Mails: Bei dieser schon länger verbreiteten Masche des **Betrugs** erhalten die Opfer eine E-Mail, die vermeintlich von Banken oder beliebten Unternehmen versandt wurde. Das Scannen der enthaltenen QR-Codes und das Eintippen persönlicher Daten sollen die vorgetäuschten Probleme lösen.

Neue Masche - Cybertrading-Betrug

Telefonbetrug:

Update vom 19. März: Kriminelle haben einen Mann im Sauerland um weit mehr als 100.000 Euro gebracht. Dabei gingen die Verbrecher besonders perfide vor:

Sie warnten selbst vor dem Betrugsversuch.

Die Betrüger schickten ihrem Opfer zunächst eine E-Mail, die wie eine Datenabfrage der Industrie- und Handelskammer (IHK) aussah. **Der Mann trug daraufhin persönliche Daten in ein Formular ein**. Am nächsten Tag rief ihn eine angebliche Bera-terin seiner Bank an und wies ihn darauf hin, **dass er auf eine betrügerische Mail der IHK hereingefallen und sein Bankkonto gehackt worden sei**. **Eine Bank ruft sie niemals an!!**

Der Mann war misstrauisch - doch die Telefonnummer im Display war offenbar sogar die seiner Bank. Im Glauben, so sein Geld schützen zu können, nannte er bereitwillig wichtige Zugangsdaten zu seinem Konto. Die Krimi-nellen nutzten diese dann, um mehr als 100.000 Euro auf ihre eigenen Konten zu überweisen. Wie kann man sich vor dieserArt Betrug schützen? **Bankdaten niemals an Fremde herausgeben**. Auch die vermeintliche Telefonnummer eines Anrufers ist gefälscht. Beim kleinsten Verdacht solle man lieber schnell **auflegen Nummer kontaktieren. und die Bank selbst unter der bekannten Nummer Kontaktieren**

Vorsicht vor falschen Amazon-Mails:

„Amazon“ behauptet, dass die letzte Zahlungsmethode nicht belastet werden konnte. Die Empfänger werden aufgefordert, ihre Zahlungsinformationen innerhalb von 48 Stunden zu aktualisieren, um eine dauerhafte Kontoschließung zu vermeiden. Laut einer Analyse sind etwa 82 Prozent dieser Fake-Mails inzwischen **KI-gestützt**. Deshalb Vorsicht!!

Außerdem: Links, die direkt in der E-Mail enthalten sind, führen nicht zur echten Amazon-Seite, sondern zu gefälschten Webseiten, die darauf abzielen, persönliche Daten zu stehlen.

Die **kurzen** Zahlungsfristen setzen den Empfänger unter Druck und können dazu führen, dass er unbedacht handelt. Die Verbraucherzentrale rät dringend davon ab, auf solche E-Mails zu reagieren. Stattdessen sollten sie umgehend in den Spam-Ordner verschoben werden.

Um sicherzugehen, dass keine echte Aufforderung übersehen wird, empfehlen die Verbraucherschützer, direkt auf **der offiziellen Website** oder in der Amazon-App nach ähnlichen Benachrichtigungen zu suchen.

Kraftfahrt-Bundesamt warnt vor betrügerischer E-Mai

Bußgeldbescheid

Sehr geehrte/r ,

Sie haben eine Geldstrafe in Höhe von **158 Euro** erhalten wegen:

• Art des Verstoßes: **Geschwindigkeitsüberschreitung**

• Datum des Vorfalls: 02/02/2025

Für Ihre Bequemlichkeit können Sie das PDF-Dokument mit den Zahlungsinformationen unter folgendem Link herunterladen:

PDF zum Download

Falls Sie mit diesem Bußgeldbescheid nicht einverstanden sind, haben Sie das Recht, innerhalb von 14 Tagen Einspruch zu erheben. Bitte kontaktieren Sie uns unter den folgenden Kontaktdaten, falls Sie Fragen haben:

1. Kraftfahrbundesamt stellt **keine** Bußgeldbescheide aus
2. Bußgeldbescheide kommen **nur per Post**
3. Keinen Link anklicken, nur ab in den Papierkorb

21.03.25

Polizei warnt vor falschem Schreiben vom Finanzamt – so erkennen Sie den Betrug

Die Betrüger schicken per Briefpost ein dreiseitiges Schreiben an das Opfer. Diese laut Polizei “**gut gemachte Fälschung im Aussehen eines Steuerbescheides**” erweckt den Anschein, dass er vom Finanzamt in Bad Salzdetfurth stammt, einer Kleinstadt in Niedersachsen. In dem Schreiben wird der Empfänger zu einer Zahlung von 762,53 Euro aufgefordert. Der Empfänger soll die geforderte Steuernachzahlung auf ein Konto bei der Sparkasse Weser-Elbe überweisen.

Bad Salzdetfurth verfügt über kein Finanzamt. Finanzämter, bei denen Betroffene nachgefragt haben, rieten den betroffenen Personen dazu, Anzeige bei der Polizei zu erstatten.

Dadurch erfuhr das LKA von dieser neuen Betrugsmasche. So sind Steuernummer und ID-Nr. auf dem Schreiben falsch. Die angegebene Telefonnummer des Finanzamtes ist nicht geschaltet und dessen Anschrift ist falsch. Der übliche Rechtsbehelf fehlt. Ein Stempel am Ende der Nachricht ist in dieser Art nicht üblich.

Rufen Sie im Zweifelsfall Ihr Finanzamt unter der Nummer an, die auf dem Steuerbescheid des Vorjahres steht. Leisten Sie keine Zahlung, sondern erstatten Sie Anzeige bei der Polizei

Polizei warnt: Betrüger missbrauchen Steuerportal Elster für Angriffe

Das LKA NDS warnt vor einer aktuellen Betrugsmasche, bei der Cybergangster unter den Namen des Steuerportals Elster.de Phishingmails mit der Adresse **Elster-Steuerinspektion@eister.de** verschicken. Die Betrüger hoffen also, dass den Empfängern nicht auffällt, dass das **“ l ”** aus Elster durch ein **“ i ”** ersetzt wurde und die Domain somit **“eister”** und nicht **“elster”** heißt, darauf hoffend, dass die Empfänger solche Details nicht erkennen. Speziell auf Smartphones mit deren kleineren Bildschirmen übersieht man solche Details leicht. In der Mail wird eine Steuerrückerstattung für das Jahr 2024 versprochen. Angeblich habe das Finanzamt den Empfänger auf dem Postweg nicht erreichen können und schickt deshalb eine Mail mit einem **grün hinterlegten Link “Zum Steuerzugang”** zu. Auf dieser Webseite soll man die für die Berechnung der Höhe der angeblichen Steuerrückzahlung **noch erforderlichen Informationen übermitteln**.

So reagieren Sie richtig

Löschen Sie diese Mail, ohne etwas darin anzuklicken. Noch besser ist es, wenn Sie diese Mail Ihrem Mailprovider als Phishingversuch melden.

27.01.2025

Europaweite Betrugsmasche "gestrandeter Touristen" mit „Bank-Apps“

Der oder die mutmaßlichen Täter sprechen Passanten an, sie brauchen z.B. dringend 1.000 Euro, haben aber kein Bargeld bei sich. Sie würden ihm in seinem Beisein zur Kontrolle stattdessen via Bank-App 1.000 Euro überweisen. Vor den Augen des Opfers täuschten sie durch Tippen am Handy in eine vermeintliche Bank-App eine Transaktion vor. Daraufhin hob das Opfer das Geld von seinem Konto ab und übergab es dem Unbekannten. Eine Gutschrift erfolgte nie. Bevorzugte Betrugsörtlichkeiten: **Bahnhöfe oder Raststätten an Autobahnen**. **Niemals dem Ersuchen nachkommen.**

02.09.2025

Auch das noch: Falsche Polizisten klingeln in „Uniform“ an der Haustür

Sie geben sich **nicht mehr nur am Telefon** als Polizisten aus - jetzt stehen sie auch noch in "Uniform" vor der Tür: In den vergangenen Tagen meldeten mehrere Bürgerinnen und Bürger aus Brackenheim (Kreis Heilbronn) versuchte Betrugsfälle durch angebliche Polizeibeamte. Besonders alarmierend: Die Täter trugen **Polizeiwesten** und zeigten gefälschte Polizei-Marken vor**. Evtl. Geldforderungen nur Online – Behörden sind nicht inkasso berechtigt!**

So klingelten am Dienstagmittag im Teilort Meimsheim zwei Männer an der Haustür einer Frau. Sie trugen augenscheinlich Polizei-Westen und behaupteten, Kriminalbeamte zu sein. Einer der Männer zeigte der Frau sogar eine Marke, die einer echten Polizeimarke zum Verwechseln ähnlich sah. Die Männer kündigten bei ihrem "Besuch" dann einen Anruf "ihres Kollegen" an, der kurz darauf tatsächlich erfolgte.

- **Vorsicht: Uniform <u>muss</u> auf der <u>linken Ärmelseite Landes/Bundes-Wappen</u> tragen, Kriminalbeamte sind in aller Regel in zivil unterwegs**

- **25.07.25**

Nicht bestellte Ware im Briefkasten

Erhalten Sie ein Paket samt Rechnung, ohne etwas bestellt zu haben, liegt entweder eine **Fehllieferung** oder eine **Betrugsmasche** vor.

Bei unseriösen Sendungen fehlt meist die Absenderadresse. Häufig handelt es sich um ***Brushing***: Betrüger nutzen dabei gestohlene Daten, schicken wahllos Ware und veröffentlichen Fake-Bewertungen unter fremden Namen. Dadurch droht, dass Ihr Profil gesperrt oder als Fake eingestuft wird.

- **Wichtige Hinweise:**
- Sie sind **nicht verpflichtet**, auf solche Lieferungen zu reagieren.
- **Keine Zahlung leisten** und **keine Daten herausgeben**.
- Ware etwa **6 Monate aufbewahren**, falls es ein Zustellfehler war und ein seriöser Händler sie zurückfordert.
- **Schutz vor Missbrauch:**
- Zwei-Faktor-Authentifizierung aktivieren
- Unterschiedliche, starke Passwörter verwenden

Unbekannte verteilen „Filmgeld“

In Osterrode (Harz) tauchten 50 Euro Scheine auf, die allesamt gefälscht waren. Es handelte sich bei diesen um sogenanntes "Filmgeld". Also „Geld“ das in Spielfilmen verwendet wird und echt wirken soll, aber ansonsten absolut wertlos ist. Wer damit im Geschäft bezahlt oder es anderweitig in Verkehr bringt, muss demzufolge nach StGB §146- 149 mit einer Strafanzeige rechnen

Die auf den ersten Blick "echt" aussehenden Scheine sind aber als „Filmgeld“ daran zu erkennen, dass das bei echtem Geld vorhandene **Wasserzeichen**, das **Hologramm** und auch der **Sicherheitsstreifen** fehlen.

Agresssive Vertreter schwätzen Ihnen neue Verträge auf

- Wenn Internet-Pishing nicht greift, versuchen es Betrüger neuerdings nach altem Rezept - direkt an der Haustür. Vertreter – häufig angeblich von der „Telekom“ – behaupten, Sie hätten schlechten Empfang und man wolle Ihnen neue, verbesserte Verträge unterbreiten. Geben Sie keine Daten über sich wie Kontonr., Bankverbindung, Geburtsdatum u.ä. heraus.
- **Vorsicht bei Haustürverträgen:**
- **Widerrufsrecht**: 14 Tage nach § 312g, § 355 BGB (schriftlich per Brief, Fax oder E-Mail). **Rückabwicklung fordern!**
- **Form**: formlos, aber eindeutig; vermeiden Sie das Wort **„Kündigung“,** verwenden Sie vielmehr das Wort **Widerruf**
- **Kein Kündigungsrecht**: Der Vertrag wird **erst nach 14 Tagen** rechtskräftig, besteht also zum Zeitpunkt der „Kündigung“ nicht
- **Folge**: vollständige Rückabwicklung, als wäre der Vertrag nie geschlossen worden.

Neue Masche vom „Finanzamt“aufgedeckt

500 Euro Strafe wegen verspäteter Steuererklärung?

Betrüger versuchen derzeit mit gefälschten Schreiben im Namen des Finanzamts, an das Geld ahnungsloser Bürgerinnen und Bürger zu gelangen.

RECHNUNG

Hinweis zur verspäteten Abgabe der Steuererklärung 2023

So erhielt eine 72-Jährige ein Schreiben, das angeblich vom Bundeszentralamt für Steuern stammte. Darin hieß es, sie habe ihre Steuerbescheinigung für das Jahr 2023 zu spät eingereicht – nun solle sie über 500 Euro als Strafe innerhalb von **zwei Tagen** überweisen.

Folgende Angabe fehlen oder sind unglaubwürdig:

Adressat, Steuernummer, Aktenzeichen bei Eintreibung einer Steuerschuld wird **grundsätzlich** eine Frist von **30 Tagen** und nicht **2 Tagen** gewährt. Ein Anruf beim Finanzamt reicht, um zu erkennen dass dies ein Fake ist. Im QR-Code verbirgt sich obendrein die Empfänger-adresse.

Und wo ist die.....natürlich im Ausland.

Kennzeichen für Deutschland ist DE und nicht ES (Spanien)

Mit postalisch zugestellten Briefen täuschen Betrüger Bankkunden über QR-Codes.

Im Kreis Böblingen erhielt ein 63-jähriger Bankkunde einen Brief mit stimmigem Briefkopf seiner „Bank“. Darin wurde er aufgefordert, seine Mobilgeräte für das Online-Banking neu einzurichten. **Der Brief wirkte echt und klang plausibel, sodass er den QR-Code scannte** und die Anweisungen mit eigens dazu erzeugten TAN‘s quittierte.

Dabei installierte er jedoch unbewusst ein Gerät der Betrüger. Diese transferierten damit Geld vom Tages-geld- auf sein Girokonto und buchten anschließend zweimal jeweils knapp 10.000 Euro ab. **01.06.2025**

Tageslimit ?

Wenn Sie von Kryptowährungen keine Ahnung haben – Finger weg

Es schien eine risikoarme Investition zu sein: Nur 300 Euro wollte ein Rentner in einer vermeintlichen Kryptowährung anlegen. Auf Grund einer im Internet geschalteten Werbeanzeige wurde ihm eine Vervielfachung seines Geldes durch geschickte Geschäfte mit Kryptowährungen angeraten.

Damit ging er einer Internet-Betrugsmasche auf den Leim. Am Ende verzeichnete er einen Verlust von mehr als 50.000 Euro, wie die Polizei mitteilte.

Dem Rentner schien dies eine sichere Sache zu sein.

Auf seinem „neuen“ bei der „Börse“ eingerichteten „Konto“ explodierte der eingezahlte Betrag förmlich. Der 78-Jährige glaubte den Zahlen, die er dort sah:

Demnach waren aus der investierten Summe bis Mai 30.000 Euro geworden. Als ein angeblicher Mitarbeiter der Kryptobörse Kontakt mit ihm aufnahm, um ihm vorgeblich den Gewinn auszuzahlen, teilte der Rentner ihm seine Bankdaten mit. Und schon war sein echtes Bankkonto geplündert: Schaden 50.000€. Abbuchung erfolgte durch eine ausländische Bank.

Investments sollten deshalb grundsätzlich nur bei Kreditinstituten abgeschlossen werden – und nicht übers Internet

Was ist „Sicherheits Telekom“ ?

Neuerdings tauchen eigenartige Schreiben der „**Sicherheits Telekom**“ auf, in denen statt des Buchstaben „**i**“(i klein) ein inverses Ausrufezeichen verwendet wird, weil die Tastaturkennung dies nicht hergibt. Das **inverse Ausrufezeichen** ist übrigens ein eigenständiges Zeichen im **Spanischen**. Es wird am Satzanfang verwendet, um eine Frage oder einen Ausruf anzukündigen.

Weiter: In dem o. angeführten Schreiben fehlen im Buchstaben „**i**“ der Punkt über dem „**i**“. Somit kann es nur von einer Maschine mit türkischer oder aserbaidschanischer Tastatur stammen.

Sie sehen, die Ganoven arbeiten weltweit gewissenhaft zusammen.

Daneben tauchen immer wieder „Steuererklärungen“ von **elster** auf, in denen durch Ersatz des Buchstabens **l(L** klein) durch **I**(i groß) angebliche Benachrichtigungen vom Finanzamt über säumige Steuern reklamiert werden. **Dies ist kaum zu erkennen!! Ihr Rechner aber erkennt das schon.** Beachten Sie dies nicht, werden Sie auf die betrügerische Seite von EISTER umgeleitet. Hier werden Sie dann in einer **„Steuer“-Abfrage** nach der ID-Nr. Ihrer Steuererklärung sowie Ihrer IBAN-Nr. gefragt, um so Ihre „verbliebene Steuerschuld“ auch umgehend begleichen zu können. In einer ähnlichen Mitteilung können Sie aber auch auf eine Steuerrückerstattung hoffen

Abhilfe schafft hier nur der Papierkorb

04.02.2025

Eine neue Betrugsmethode
Recovery-Scam

Wenn Betrüger zweimal zuschlagen: Das beschreibt den sogenannten „**Recovery Scam“**. Nach einem ersten Betrug winkt dem Opfer plötzlich Rettung und die Hoffnung, doch noch das verlorene Geld zurückzubekommen.

Zunächst erwerben die Betreiber dieser Callcenter Datenbestände im DarkNet Kontaktdaten von Geschädigten, welche bereits in der Vergangenheit Verluste durch eine andere betrügerische Anlageplattformen erlitten hatten. **Das Opfer wird von einer angeblichen „Kanzlei“ oder „Fachabteilung“ kontaktiert. Man bietet Hilfe an.**

Die Täter seien ermittelt, das Konto der Betrüger sei eingefroren worden, und das Geld könne zurückgeholt werden. Dazu muss die Firma nur beauftragt werden. Und die arbeitet natürlich nicht ehrenamtlich. Damit das gerettete Geld dann später ausbezahlt werden kann, wird natürlich noch eine Gebühr fällig. Bis am Ende auch das weg ist.

Telekom-Betrug: Verbraucherzentrale warnt vor verdächtiger E-Mail

Die Verbraucherzentralen warnen vor einem aktuellen **Phishing-Angriff auf Telekom-Kunden**. Die fragliche E-Mail sieht auf den ersten Blick echt aus: Die „Telekom“ weist in einer „automatisch“ generierten Nachricht darauf hin, dass man einen Anruf verpasst habe und eine Sprachnachricht auf der Mailbox hinterlassen wurde. Diese könne man über den **Link** der E-Mail abhören. Der Betreff lautet **"[Telekom]- Voicemail hinterlassen von +49 XXX XXXXXX**". Bei der Telefonnummer handelt es sich um **eine einfache achtstellige Zahlenfolge**, die mit großer Wahrscheinlichkeit zufällig generiert wurde.

Weitere Anzeichen finden sich bei der unpersönlichen Anrede mit "Sehr geehrte(r) Kunde/Kundin" sowie dem weiterführenden Link. Anstatt einer offiziellen Telekom-Adresse findet man **als Absender die Privatadresse eines T-Online-Nutzers**. Obendrein fehlt das Logo der Telekom, das sonst in E-Mails des Unternehmens auftaucht. **Über Nachrichten auf der Mailbox werden Telekom-Kunden in der Regel per SMS** oder in einer Voicemail-App benachrichtigt - **nicht per E-Mail.**

Ein guter Weg, den Betrug zu erkennen, sei der Betreff. Hier sollte bei einer **echten eMail der Telekom das Buchungskonto, Kundenkonto (bei Rechnungen und Mahnungen) oder die Zugangsnummer (bei Nachrichten des Sicherheitsteams)** in der Betreffzeile stehen

01.03.2025

Identitätsbetrug !!!

Sie sind einem Phishing-Angriff erlegen. Auf eine eMail Ihrer **„Bank“** haben Sie zur angeblichen **Verifizierung** Ihrer Person **(bei diesem Begriff läuten bei mir alle Alarmglocken)** neben persönlicher Daten, wie Übermittlung des PA, Bankdaten wie IBAN, Passwörter, „Foto-TAN“ usw. preisgegeben. **Damit nimmt der Betrüger Ihre Identität an**. Seine erste Handlung wird die Änderung Ihres Passworts als Zugang zu Ihrem Online-Konto sein. Er sperrt Sie aus, damit er in Ruhe Ihr Konto abräumen kann. Im nächsten Schritt tätigt er z.B. Bestellungen mit einem Weiterleitungs-vermerk. Die Rechnungen gehen an Sie. Mahnungen! Im Gefolge werden Inkasso-Unternehmen und Gerichte bemüht. Auch Anlage neuer Konten, Kreditanträge sind möglich, aber wohl schwieriger zu erlangen. **In allen Fälle sind Sie beweispflichtig** und wissen nichts von den Machenschaf-ten des Betrügers. Ihre Daten können auch im DarkNet zur weiteren Verfügung verkauft werden. Es ist beunruhigend, wenn Sie feststellen, Opfer eines Identitätsbetrugs geworden zu sein. Im Extremfall kann sogar Ihre ganze Existenz gefährdet sein. **Deshalb informieren Sie unverzüg-lich Ihre Bank und erstatten umgehend Anzeige bei der Kriminal-polizei!!!**

Auf jeden Fall werden Sie mindestens unheimlichen Ärger und evtl. finanzielle Einbussen über Schadensersatzforderungen haben.

Bußgeldbescheide per eMail

Betrügerische Bußgeldbescheide sind groß in Mode. Sie sollen Menschen verunsichern und Geldzahlungen ergaunern. Die gefälschten Bescheide sehen echten amtlichen Schreiben **täuschend ähnlich** und enthalten Drohungen wie Mahngebühren oder Vollstreckungsmaßnahmen, um Druck aufzubauen.

Wie erkennt man einen gefälschten Bußgeldbescheid?

Absender prüfen: **Echte Bußgeldbescheide** kommen von offiziellen Behörden (Ordnungsamt, Polizei) und ***nicht per eMail***. Prüfen Sie die Adresse und Kontaktdaten.

IBAN & Zahlungsaufforderung: an Konten mit „**DE“-IBAN** zwingend, da **deutsche Behörde**

Rechtschreibung & Layout: Fehlerhafte Grammatik, untypische Schriftarten oder Formulierungen sind verdächtig.

Fehlende Rechtsmittelbelehrung: Ein echter Bußgeldbescheid enthält **Hinweise zur Einspruchsmöglichkeit.**

Ungewöhnliche Verstöße: Wenn Sie sicher sind, zur angegebenen Zeit nicht am Ort des Verstoßes gewesen zu sein.

Nicht zahlen

Bei Betrug Polizei informieren.

Vermeiden Sie diese Fehler beim Bezahlen mit der Geldkarte

Im Alltag geht das Bezahlen mit der Bankkarte oft schnell und routiniert – doch gerade dann schleichen sich leicht unbemerkte Fehler ein, deshalb um sich vor Sicherheitsrisiken zu schützen, achten Sie auf:

- **1. PIN und Karte nie beieinander**
- **2. Unaufmerksamkeit bei der PIN-Eingabe in der Öffentlichkeit**
- **3. Ablenkung durch Fremde**
- **4. Unsachgemäße lose Aufbewahrung**

Reduzierung telefonischer Belästigungen

Telefonische Belästigungen können Sie durch Antrag bei Ihrem Telefonbetreiber zur Löschung Ihrer persönlichen Einträge im Telefonbuch und auch im Internet **wenigstens reduzieren**. Hier muss ausdrücklich darauf hingewiesen werden, dass u.U. auch Einträge in Internet durch Ihren Telefonbetreiber ohne Ihr Wissen vorgenommen worden sein können. Eine lukrative Einnahmequelle, denn Einträge lassen sich bestens weiterverkaufen – von Händler zu Händler - oder sogar im DarkNet anbieten.

Sie fragen sich, wie Betrüger immer wieder und ausgerechnet an Ihre Telefonnummer gelangen. Nichts einfacher als das! Vornamen wie z.B. Edelgard, Rotraut, Irmingard bzw. Teutobod, Sigurd, Treugott lassen drauf schließen, dass Sie eine Spezies älteren Semesters sind und sich bestens für Betrügerattacken eignen. Auch kurze Telefonnummern können ein Hinweis sein, dass sie u.U. schon älter sind. Also Eintrag löschen. Wenn Sie auch weiterhin auf Ihren Telefonbucheintrag bestehen, so „verunstalten“ Sie wenigstens Ihren Vornamen durch Setzen nur eines Buchstabens, gefolgt von einem Punkt. **A.** ist wenig aussagekräftig ob Sie männlichen oder weiblichen Geschlechts sind und lässt auch keine Rückschlüsse auf Ihr Alter zu. Und das soll auch wenigstens Sinn und Zweck der Sache sein.

Persönliche Daten niemals an Unbekannte weitergeben, keinen Geldforderungen nachkommen !

- **1. Bei unbekannter Tel-Nr nur mit „Hallo“ melden**
- **keinen Namen nennen, erst recht nicht mit “Ja“ antworten**
- **2. Ihr Geburtsdatum**
- **3. Ihre Iban-Nummer (Konto-Nr), keine TAN abrufen**
- **4. Ihr Passwort**
- **5. Strom-Zählernummer (Nr. existiert nur 1x in BRD)**
- **6. Keine Geldgeschäfte per Telefon (z.B. Bitcoin, Bank)**
- **7. Niemals Geld herausgeben, auch nicht an die „Polizei“**
- **und erst recht nicht an der Haustüre**
- **8. Geldforderungen per eMails, WhatsApp und SMS nie beachten,**
- **Anhang von Mails nicht öffnen, nur löschen**
- **9. Keine Übermittlung von Foto-TAN oder FingerPrint; PA**

Daten (1-5) leiten Sie **NIEMALS** an Unbekannte weiter, ansonsten ermöglichen Sie Buchungen von Ihrem Konto, bzw. wechseln z.B. den Stromanbieter(Pkt.2, 5) **ohne** Ihr Wissen. Dies ist ein **ehernes Gesetz!**

Betrug per Lastschrift: So können sich Verbraucher schützen

Das Europäische Verbraucherzentrum Deutschland mit den Tipps

- Kein Geld verschenken: Prüfen Sie **regelmäßig** Ihre Kontoauszüge.
- Bemerken Sie auffällige oder unberechtigte Abbuchungen, **beanstanden** Sie diese direkt **beim betreffenden Unternehmen**.
- Wenn Sie vermuten, dass Ihre Daten missbräuchlich verwendet wurden, setzen Sie sich umgehend mit Ihrer Bank in Verbindung und lassen Sie **Ihr Konto und Ihre Karte sperren.**
- Bei unberechtigte Abbuchungen können Sie innerhalb von acht Wochen die Lastschrift von Ihrer Bank **zurückbuchen** lassen.
- Black-Listing: Kommt es wiederholt zu unberechtigten Abbuchungen, können Sie **Ihr Konto** bei Ihrer Bank **für Abbuchungen des Unternehmens sperren lassen.**
- **Tageslimit für Kontotransaktionen einrichten:** Damit verhindern Sie, dass Ihr Konto einfach „leergeräumt werden kann“. Und Sie behalten dadurch auch einen besseren Überblick.