



# Mehr Sicherheit

Seien Sie wachsam! Im Internet, am Telefon oder unterwegs: die besten Tipps gegen Trickbetrug.



**Sparda-Bank**

Sparda-Bank Hessen eG

# Betrugsfälle häufen sich

Kriminelle entwickeln immer neue Maschen, um ihre Opfer zu täuschen – und haben damit oft Erfolg, wie aktuelle Daten zeigen. Umso wichtiger ist es, sich zu schützen.

## Cybercrime: Taten nehmen zu

Laut aktuellem Bundeslagebericht „Cybercrime“ ist im Jahr 2023 die Anzahl der Straftaten im Bereich „Auslandstaten Cybercrime“ um rund 28 Prozent im Vergleich zum Vorjahr gestiegen. Gemeint sind damit Fälle, bei denen in Deutschland Schäden entstehen, der Aufenthaltsort der Täter aber im Ausland liegt oder unbekannt ist.



**97.327**  
**Beschwerden**

## Betrugsversuche per Textnachricht

Im Jahr 2023 gingen bei der Bundesnetzagentur 97.327 Betrugs(versuchs)meldungen ein, die sich auf Spam und Einzeltrickfälle per SMS und Messengerdienste beziehen.



## Großteil der Internetnutzer betroffen

Laut einer Umfrage des Digitalverbands Bitkom sind im Jahr 2023 rund 67 Prozent der Internetnutzer Opfer von Cyberkriminalität geworden. 35 Prozent waren von Phishing betroffen.



Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern die männliche Sprachform verwendet. Entsprechende Begriffe gelten grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat rein redaktionelle Gründe und beinhaltet keine Wertung.



## Lassen Sie sich nicht unter Druck setzen!

Sie verlangen eine Kaution, um die angebliche Haft eines Angehörigen zu vermeiden oder, oder, oder. Trickbetrüger verstehen es, Angst zu machen. Nicht mit Ihnen!

Gehört haben Sie bestimmt schon mal von diesen Betrugsvarianten: Enkeltrick, falsche Polizisten am Telefon, betrügerische WhatsApp-Nachrichten, Schockanrufe von angeblichen Verwandten. Wenn man erst mal selbst so einen Anruf erlebt, ist die Verunsicherung groß. Daher lautet der wichtigste Rat der Polizei: Bleiben Sie ruhig und lassen Sie sich nicht unter Druck setzen! Das klingt vielleicht einfacher, als es in der Situation ist. Aber sofern Sie nicht gleich auflegen, denken Sie immer daran: Fühlen Sie

sich bedrängt und fordert der Anrufer Wertgegenstände, sensible Daten oder Informationen zu Ihren Vermögensverhältnissen, handelt es sich mit Sicherheit um einen Betrugsversuch. Zögern Sie dann nicht und legen Sie einfach auf! So können Sie sich kurz Notizen machen und anschließend die 110 wählen, um der Polizei den Sachverhalt zu schildern.

Unser Überblick auf den nächsten Seiten fasst die wichtigsten Infos zu verbreiteten Betrugsmaschinen zusammen.



### WhatsApp-Tipp

Erhöhen Sie die Sicherheit Ihrer Nachrichten, Anrufe und Daten in WhatsApp. Wählen Sie in der App „Einstellungen“ aus und tippen Sie dann auf „Datenschutz“. Dann starten Sie den Datenschutz-Check und legen Ihre Einstellungen fest.



Hallo Mama, rate mal, wessen Handy in der Waschmaschine gelandet ist. Du kannst diese Nummer einspeichern und die alte löschen 😞

19:30

### Checkliste Enkeltrick

- ✓ **Misstrauisch sein:** Fordern Sie Anrufer und SMS-/Messengerkontakte immer dazu auf, ihren Namen zu nennen, und lassen Sie sich nicht dazu drängen zu raten.
- ✓ **Wissen prüfen:** Erfragen Sie Dinge, die nur echte Verwandte/Bekannte wissen können.
- ✓ **Zeit nehmen:** Rufen Sie Ihre Verwandten unter der Ihnen bekannten Rufnummer an und lassen Sie sich den Sachverhalt bestätigen.
- ✓ **Rat suchen:** Holen Sie Vertraute ins Boot und schildern Sie verdächtige Anrufe oder Nachrichten. So fällt ein Betrug schnell auf.

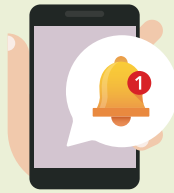
### Enkeltrick: So schützen Sie sich

Der sogenannte Enkeltrick ist ein Klassiker unter den Betrugsmaschen. Mal geben sich Kriminelle als Enkelkinder älterer Menschen aus und setzen die Betroffenen am Telefon unter Druck. Mal nutzen sie andere Kanäle wie SMS und Messengerdienste. Hier geben sie sich als nahe Verwandte aus, bauen ein Vertrauensverhältnis auf – und fordern schließlich Geld. Doch es gibt Möglichkeiten, sich zu schützen.

#### Der Rat der Polizei

Lassen Sie sich nicht unter Druck setzen. Beenden Sie das Gespräch bzw. den Chat.





## Achtung, Anruf: Misstrauen ist der beste Schutz

Die verweinte Stimme eines „Verwandten“, ein „Polizist“ oder sogar „Interpol“ am Telefon – und immer die gleiche Masche: den

Angerufenen unter Druck setzen, in ein Gespräch verwickeln, die Verunsicherung ausnutzen und zu Geldzahlungen bewegen. Machen Sie sich bewusst: Es handelt sich um Betrug und Ihre Hilfsbereitschaft soll ausgenutzt werden.

**Der Rat der Polizei:** Legen Sie auf – und überweisen oder übergeben Sie nie Geld oder Wertgegenstände! Weder die Polizei noch die Staatsanwaltschaft würde am Telefon Geld von Ihnen fordern.



## WhatsApp-Nachrichten: Vorsicht bei unbekanntem Nummern

An den Austausch von Nachrichten mit Freunden oder der Familie über Messengerprogramme wie WhatsApp, Threema oder

Signal haben wir uns längst gewöhnt. Wachsamkeit ist aber wichtig, wenn plötzlich eine Nachricht mit einer Anrede wie „Hallo Mama! Hallo Papa!“ von einer unbekanntem Rufnummer erscheint. Folgt dann kurz darauf noch die Bitte, Geld für einen Notfall zu überweisen, sollten Sie alarmiert sein.

**Der Rat der Polizei:** Blockieren Sie die Nummer. Wurden Geldforderungen gestellt, machen Sie Screenshots des Chats und melden Sie den Vorfall der Polizei.



## Falscher Mitarbeiter am Telefon: Auflegen ist die richtige Wahl

„Sie haben die neueste Windows-Version noch nicht installiert? Dann helfe ich Ihnen gern weiter.“ So oder ähnlich melden sich z.B. immer

wieder angebliche Microsoft-Mitarbeiter am Telefon. Vergleichbares erlebt man mit falschen Bankmitarbeitern, die etwa verlangen, dass Sie angebliche Testüberweisungen per App freigeben. Diese Anrufe (mitunter auch E-Mails) haben immer das gleiche Ziel: Zugriff auf Ihren Computer zu bekommen, um etwa Passwörter oder Kreditkartendaten auszuspähen.

**Der Rat der Polizei:** Lassen Sie sich auf kein Gespräch ein und beenden Sie den Anruf sofort. Sie haben es mit Betrügern zu tun.

### Checkliste Telefonanrufe

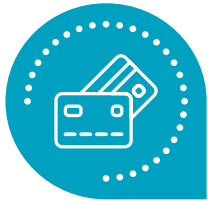
- ✓ **Nicht unter Druck setzen lassen** und niemals Geld überweisen.
- ✓ **Nur mit „Hallo“ melden**, wenn die Rufnummer nicht bekannt ist.
- ✓ **Nicht zurückrufen**, wenn Sie die angezeigte Nummer nicht kennen.
- ✓ **Die jeweilige Person anrufen** – und zwar unter einer Ihnen bekannten Nummer – und den Sachverhalt bestätigen lassen.

### Checkliste Chatbetrug

- ✓ **Keine unbekanntem Nummer aufnehmen** in die WhatsApp-App-Liste. Überprüfen Sie die Identität unter einer Ihnen bekannten Nummer.
- ✓ **Überweisen Sie niemals Geld**, wenn Sie per Nachricht darum gebeten werden.
- ✓ **Schützen Sie Ihr Profilbild** bei WhatsApp und machen Sie es nur für gespeicherte Kontakte sichtbar.

### Checkliste Mitarbeiter

- ✓ **Das Gespräch sofort beenden.** Kein echter Microsoft-Mitarbeiter ruft unaufgefordert Kunden an.
- ✓ **Keine Fremdprogramme installieren** auf Ihrem PC, Tablet oder Smartphone.
- ✓ **Nicht auf Drohungen reagieren**, wenn die Person behauptet, dass Ihre Windows-Version gelöscht wird.



# Sicher bezahlen im Internet

Internetbetrüger legen sich ins Zeug, um an Ihre Zahlungs- und Login-Daten zu kommen. Wir erklären, wie Sie Kriminellen nicht ins Netz gehen.



## Ist dieser Online-Shop seriös?

Lassen Sie sich von Superschnäppchen nicht blenden, sondern prüfen Sie, ob es sich tatsächlich um einen seriösen Online-Händler handelt – unter

[verbraucherzentrale.de/fakeshopfinder](https://www.verbraucherzentrale.de/fakeshopfinder)



Das Ziel von Kriminellen im Netz ist immer das gleiche: sensible Informationen wie Zahlungs-, Konto- oder Login-Daten zu ergaunern, um an Ihr Geld zu kommen. Zu den verbreiteten Märschen gehören etwa seriös auftretende Online-Shops, täuschend echt aussehende E-Mails und QR-Codes, die dazu verleiten, auf Links zu klicken und sensible Daten preiszugeben. Mit aufmerksamem Verhalten im digitalen Alltag können Sie sich aber grundsätzlich vor Fake-Shops und Co. schützen.

Insbesondere bei Bezahlvorgängen im Internet ist Aufmerksamkeit geboten. Denn Kriminelle suchen immer neue Zugangswege, um an Ihre Zahlungsdaten zu gelangen.

### Am besten auf Rechnung kaufen

Wenn möglich, sollten Sie Online-Einkäufe auf Rechnung bezahlen, so die Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI). So stellen Sie sicher, dass Sie die Ware erst dann bezahlen, wenn sie



## Seien Sie achtsam bei QR-Codes!

Immer häufiger nutzen Kriminelle QR-Codes, um Nutzer auf Websites zu locken und vertrauliche Informationen zu stehlen (Quishing). Diese QR-Codes können in E-Mails, auf Flyern, in sozialen Medien oder auf Websites eingebettet sein.

### Seien Sie wachsam!

Scannen Sie nur QR-Codes von vertrauenswürdigen Quellen. QR-Codes aus unbekanntem oder verdächtigen E-Mails, Nachrichten oder Websites besser nicht nutzen.

## Checkliste QR-Codes

- ✓ **Seien Sie skeptisch.** Scannen Sie nur QR-Codes aus vertrauenswürdigen Quellen.
- ✓ **Bevor Sie die Website besuchen, prüfen Sie die URL sorgfältig.** Sie wird Ihnen nach dem Scannen angezeigt. Achten Sie auf verdächtige oder ungewöhnliche Zeichenfolgen.
- ✓ **Vorsicht an öffentlichen Orten:** Betrügerische QR-Codes finden sich oft auch in vermeintlich harmlosen Beiträgen auf Plakaten und Co., um Ihre Neugier zu wecken.

geliefert wurde. Zudem geben Sie Ihre Zahlungsdaten nicht an Dritte weiter.

### Kreditkartenzahlung ist auch geeignet

Auch die Kreditkartenzahlung bietet aufgrund der Zwei-Faktor-Authentifizierung ein hohes Maß an Sicherheit. Ganz wichtig: Prüfen Sie die Seriosität des Online-Shops genau, bevor Sie Ihre Kartendaten eingeben.

### Lastschrift: Sie können widersprechen

Oft besteht auch die Möglichkeit, per Lastschrift zu bezahlen. Dabei übermitteln Sie Ihre Kontodaten (IBAN/BIC) an den Online-Shop und geben durch das Erteilen eines SEPA-Mandats die Erlaubnis, den Rechnungsbetrag von Ihrem Konto einzuziehen. Der Vorteil: Sie können der Einzugsermächtigung innerhalb von acht Wochen nach Einzug des Rechnungsbetrags widersprechen. Da Sie auch hier Ihre Kontodaten beim Bezahlen eingeben müssen, ist Vorsicht geboten.

### Vorsicht bei Online-Zahlungsdiensten

Sehr verbreitet sind auch Online-Zahlungsdienste. Hier hinterlegen Sie Ihre Kontodaten vorab in einem Kunden-

konto. Beim Bezahlvorgang müssen Sie dann nicht mehr Ihre Kontodaten eingeben. Umso wichtiger ist es, das Kundenkonto vor Fremdzugriffen zu schützen. Denken Sie auch daran, in den Einstellungen des Anbieters die Zwei-Faktor-Authentifizierung zu aktivieren. So können keine Zahlungen ohne vorherige Bestätigung getätigt werden. Mehr dazu auf Seite 10.

Denken Sie daran: Sollten Betrüger Ihre Bank-, Kreditkarten- oder Kontodaten haben, lassen Sie Ihre Zugänge und Karten sofort sperren! Die Sperrnummern für BankCard und Mastercard® finden Sie rechts auf dieser Seite.

### Vorsicht bei Kleinanzeigen

Besondere Aufmerksamkeit ist beim Kaufen und Verkaufen auf Kleinanzeigenplattformen gefragt. Grundsätzlich gilt: Informieren Sie sich vor jeder Transaktion immer über aktuelle Warnhinweise und geben Sie niemals Ihre Kontodaten preis! Sie wickeln Privatkäufe gern über Online-Zahlungsdienste ab? Dann prüfen Sie vorab, ob Ihr Anbieter einen Käuferschutz bietet und wie weit dieser reicht.



**Diese Sperrnummern sollten Sie sich notieren!**

Melden Sie einen Missbrauch Ihrer Konto- bzw. Kartendaten, auch wenn Sie nur einen Verdacht haben, sofort unter

**BankCard** (Debitkarte)  
**116 116** (kostenfrei)

**Mastercard®**  
(Kreditkarte)  
**069 6657 1919**

## Checkliste Fake-Shops

- ✓ **Überlegen Sie, ob der Preis realistisch ist** oder das Angebot eigentlich zu gut ist, um wahr zu sein.
- ✓ **Klicken Sie auf das Impressum**, ganz unten auf der Internetseite. Finden Sie keines, heißt es besser: Finger weg!
- ✓ **Überprüfen Sie die Seriosität der Internetseite.** Suchen Sie dafür mit deren Namen in einer Suchmaschine nach möglichen Warnhinweisen und Kundenrezensionen.
- ✓ **Wählen Sie als Zahlungsoption nicht „Vorkasse“ oder „Sofortüberweisung“.** Es sollte auch andere Zahlungsmöglichkeiten geben. Auch eine Widerrufsbelehrung muss da sein.

## Checkliste Phishing

- ✓ **Löschen Sie E-Mails**, wenn Sie darin zur Eingabe persönlicher Daten wie Passwörtern oder Kundendaten aufgefordert werden.
- ✓ **Klicken Sie nicht auf Links**, die in Nachrichten von vermeintlichen Banken oder Unternehmen enthalten sind. Melden Sie sich direkt in Ihrem Nutzerkonto an und prüfen Sie dort, ob es Nachrichten für Sie gibt.
- ✓ **Überprüfen Sie die Adresszeile des Webbrowsers.** So erkennen Sie, ob es sich um die richtige Website handelt.
- ✓ **Richten Sie Favoriten in Ihrem Webbrowser ein.** So verwenden Sie nur die offiziellen Zugänge für Ihre Bankgeschäfte.



## So shoppen Sie sicher im Internet

Egal ob Markenkleidung, Fotoausrüstung, Smartphone oder Parfüm: Die Versuchung, sich auf

der Shoppingtour im Internet mit wenigen Klicks einen verlockenden Schnäppchenpreis zu sichern, ist groß. Hier sollte der gesunde Menschenverstand aber erst mal „Stopp“ sagen. Denn es kann richtig teuer werden, wenn Sie dabei auf einen sogenannten Fake-Shop hereinfallen. Hinter den vermeintlichen Online-Shops stehen Kriminelle. Bestellen Sie hier, ist Ihr Geld weg und Ihre Ware bekommen Sie auch nicht.

### Vor dem Kauf den Preis vergleichen

Bei allzu verlockenden Angeboten kann ein Vergleich Klarheit schaffen. Sind die Preise für das Produkt gegenüber den bekannten Vergleichsportalen deutlich niedriger, spricht das fast immer für Betrug. Nutzen Sie auch den Fake-Shop-Finder der Verbraucherzentrale: Hier können Online-Shops auf Merkmale eines Fake-Shops überprüft werden.



## Vorsicht, Phishing: Daten nicht an den Haken geben

Die wichtigste Regel zum Schutz vor Datendieben lässt sich ganz einfach merken: Ihre Sparda-

Bank Hessen oder auch ein anderes Bankinstitut fordert Sie niemals per E-Mail zur Eingabe Ihrer vertraulichen Bankdaten wie Benutzername oder Passwort auf! Falls Sie eine solche E-Mail erhalten, lassen Sie sich von der vermeintlichen Echtheit nicht täuschen – löschen Sie diese sofort aus Ihrem Postfach. Die Absender haben es auf Ihre Zugangsdaten abgesehen!

### Webadresse auf Echtheit prüfen

Sichere Internetseiten, auf denen Sie Ihre sensiblen Daten eingeben müssen, erkennen Sie an den Buchstaben „https://“ in der Adresszeile und an einem Schloss- oder Schlüsselsymbol im Internetbrowser. Mit einem Klick auf das Schlosssymbol können Sie die Echtheit prüfen.





# Bankgeschäfte sicher erledigen

Wir bieten modernes Online-Banking mit höchsten Sicherheitsstandards sowie zeitgemäße Apps. So erledigen Sie Ihre Bankgeschäfte sicher, einfach und schnell.



Eine Sache ist sicher: Mit dem Online-Banking der Sparda-Bank Hessen erledigen Sie Ihre Bankgeschäfte jederzeit sicher und sorgenfrei. Alle unsere Systeme und Programme sind nach dem aktuellen Stand der Technik abgesichert. Mit ständigen Weiterentwicklungen, Tests und moderner Technik gewährleisten wir einen hohen Sicherheitsstandard für

unsere Kunden und Mitglieder. So können Sie z.B. mit unserer Freigabe-App ohne TAN-Eingabe Ihre Online-Banking-Transaktionen wie Überweisungen, Serviceaufträge oder Daueraufträge schnell und sicher auf Ihrem Smartphone bestätigen. Zudem bietet die Nutzung unserer Apps ein hohes Maß an Sicherheit für alle Transaktionen. >

### Doppelt gesichert hält besser

Für das sichere Abwickeln Ihrer Bankgeschäfte steht Ihnen die sogenannte Zwei-Faktor-Authentifizierung zur Verfügung. Dieses Schutzverfahren bestätigt Ihre Identität aus zwei unterschiedlichen Quellen. So können Sie sich vor Fremdzugriffen auf Nutzerkonten und Identitätsdiebstahl schützen. Im Kasten

unten erfahren Sie, wie das Verfahren funktioniert.

### Wir halten Sie auf dem Laufenden

Auf unserer Website veröffentlichen wir laufend Sicherheitshinweise und Warnungen zu aktuellen Betrugsmaschen. Schauen Sie regelmäßig vorbei! [sparda-hessen.de/warnhinweise](https://sparda-hessen.de/warnhinweise)



So können Sie Ihren Online-Banking-Zugang sperren

#### Telefonisch

069 7537-0  
(Mo. bis Fr.:  
8:00–18:00 Uhr)

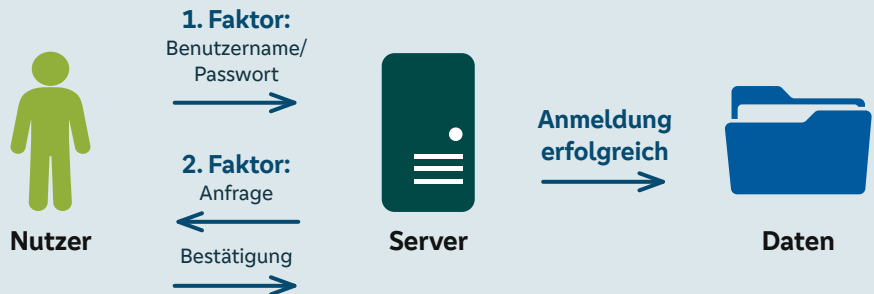
#### Online-Banking

Klicken Sie auf „Sicherheit“ und wählen Sie „Zugang verwalten“.

#### Banking-App

Tippen Sie auf den Menüpunkt „Meine Banken“ und wählen Sie „Banking sperren“.

## Zwei-Faktor-Authentifizierung: Das steckt hinter dem Sicherheitsverfahren



### Der Prozess

Die Zwei-Faktor-Authentifizierung beginnt in der Regel mit der Eingabe der persönlichen Zugangsdaten. Sie sind in dem zweistufigen Prozess der 1. Faktor, mit dem sich der Nutzer identifiziert. Das System bestätigt daraufhin die Richtigkeit der eingegebenen Zugangsdaten. Im nächsten Schritt muss der Nutzer seine Identität bestätigen. Diese Abfrage ist der 2. Faktor im Authentifizierungsprozess und geschieht durch ein vorab festgelegtes Freigabeverfahren.

### Der Vorteil

Mit der zweistufigen Authentifizierung wird vermieden, dass Dritte, die an Ihre Zugangsdaten gelangt sind,

sich allein mit diesen einloggen und über Ihr Konto verfügen können.

### Unser Standard

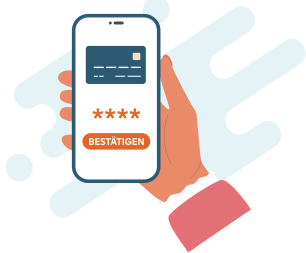
Auch das Online-Banking Ihrer Sparda-Bank Hessen ist durch die Zwei-Faktor-Authentifizierung geschützt: Alle 90 Tage bestätigen Sie Ihren Login und grundsätzlich jeden Auftrag durch das von Ihnen gewählte Freigabeverfahren.

Für Kreditkartenzahlungen, die Sie online tätigen, steht Ihnen der Mastercard® Identity Check™ zur Verfügung. Beim Bezahlvorgang öffnet sich Ihr SpardaOnline-Banking und Sie bestätigen die Zahlung einfach mit dem von Ihnen gewählten Freigabeverfahren.



## Das können Sie tun

Auch Sie selbst können einiges dafür tun, für mehr Sicherheit zu sorgen. Wir haben ein paar Tipps für Sie zusammengestellt.



### Auch unterwegs achtsam sein

Nicht immer brauchen Betrüger ausgefeilte Methoden, um an sensible Daten zu kommen. Beim „Shoulder Surfing“ schauen Ihnen Kriminelle über die Schulter und versuchen so, Daten auszuspähen. Schützen Sie daher unbedingt am Geldautomaten und beim Bezahlen immer die Eingabe Ihrer PIN mit der freien Hand. Vorsicht ist auch geboten, wenn Sie unterwegs mal eben eine Buchung oder einen Online-Kauf erledigen möchten. Schützen Sie Ihre Zugangsdaten vor neugierigen Blicken.



### Mit Sicherheit gut beraten!

Schon gewusst? Die Polizeiliche Kriminalprävention bietet kostenlose Beratung – auch zu Betrugsthemen. Mehr unter

**polizei-beratung.de**



### Nicht auf unbekannte E-Mails reagieren

Ganz wichtig: Kein Unternehmen, bei dem Sie ein Kundenkonto besitzen, würde Sie jemals per E-Mail, SMS oder Anschreiben dazu auffordern, Ihre Zugangsdaten „zu bestätigen“. Öffnen Sie daher bitte auch niemals einen Link in einer E-Mail, wenn Sie den Absender nicht kennen. Fragen Sie im Zweifel immer lieber direkt über die Ihnen bekannten Erreichbarkeiten nach!



### Auf IT-Sicherheit achten

Wie können Sie selbst für mehr Sicherheit sorgen? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein paar grundsätzliche Empfehlungen: Halten Sie Ihre Software durch Updates immer auf dem neuesten Stand. Verwenden Sie möglichst starke und unterschiedliche Passwörter. Nutzen Sie ein aktuelles Virenschutzprogramm und eine Firewall.

# Diese Regeln gelten immer

Auf den vorherigen Seiten finden Sie für jede vorgestellte Betrugsmasche eine eigene Checkliste. Zudem gibt es ein paar Grundregeln, die Sie in jedem Fall beachten sollten.

## 1. Nicht unter Druck setzen lassen

Vorsicht bei Anrufen von Fremden! Sagen Sie, dass es gerade ungünstig ist, und bieten Sie einen Rückruf an. Reagiert der Anrufende nicht und will Sie in ein Gespräch verwickeln, beenden Sie das Telefonat sofort.

## 2. Immer nach dem Namen fragen

Gibt sich jemand an der Haustür oder am Telefon z. B. als Polizeibeamter aus, fragen Sie direkt nach dem Namen. Schließen Sie die Tür oder legen Sie auf, wählen Sie 110 und schildern Sie der echten Polizei den Vorfall.

## 3. Bei verdächtigen Anrufen auflegen

Vertrauen Sie auf Ihr Gefühl und beenden Sie Telefonate sofort, wenn Ihnen etwas komisch erscheint. Ein schlechtes Gewissen brauchen Sie dabei nicht zu haben. Sie sind keineswegs unhöflich.

## 4. Nie Geld oder Wertsachen übergeben

Unbedingt beachten: Übergeben Sie nie Geld oder Wertsachen an Unbekannte! Die Polizei wird Sie niemals dazu auffordern, Geld oder Wertsachen herauszugeben.

## 5. Niemals Login-Daten herausgeben

Ihre Daten gehören nur Ihnen. Geben Sie sensible Bankdaten wie Ihre PIN oder TAN und andere Kontodaten niemals an Dritte weiter.

### Impressum

**Herausgeber:** Sparda-Bank Hessen eG, Medien- und Öffentlichkeitsarbeit

**Sitz der Genossenschaft:** Osloer Straße 2, 60327 Frankfurt am Main

**Service-Telefon:** 069 7537-0

**Web-Adresse:** sparda-hessen.de

**E-Mail:** kontakt@sparda-hessen.de



### Wir sind für Sie da!

Sie erhalten verdächtige E-Mails, Anrufe oder SMS? Dann nehmen Sie bitte Kontakt zu uns auf. Wir unterstützen Sie gern!

[sparda-hessen.de](https://www.sparda-hessen.de)

