



# Mehr Sicherheit

Lassen Sie sich nicht ködern! Im Internet, am Telefon oder an der Haustür: die besten Tipps gegen Trickbetrug von Ihrer Sparda-Bank Südwest.

**Sparda-Bank**



**Diese Sperrnummern sollten Sie sich notieren!**

Melden Sie einen Missbrauch Ihrer Konto- bzw. Kartendaten sofort unter

girocard (Debitkarte) 116 116 (kostenfrei)

Mastercard® (Kreditkarte) 0721 120 966 001

Sperrung des Online-Bankings im geschützten Bereich des Online-Bankings oder telefonisch unter 06131 63 63 63 (Mo–Fr: 6 bis 22 Uhr; Sa: 9 bis 16 Uhr)



Hier gibt's alle Nummern auf einen Blick!



**„WIR SIND VON MENSCH ZU MENSCH FÜR SIE DA.“**

**Tobias Meurer**  
Mitglied des Vorstands  
der Sparda-Bank Südwest eG

**A**ls Genossenschaftsbank gehören wir unseren Mitgliedern. Sie zu fördern, ist der Zweck unseres Unternehmens. Das bedeutet zum Beispiel auch, unsere Kundinnen und Kunden bestmöglich bei der Betrugsprävention zu unterstützen. Für unsere Services setzen wir daher auf hohe Sicherheitsstandards und modernste Technologie.

Kriminelle entwickeln allerdings immer neue Tricks, um an sensible Informationen wie etwa Kontodaten zu kommen. Dazu zählen sogenannte Schockanrufe, bei denen Täter ihre Opfer massiv unter Druck setzen. Und wahrscheinlich haben Sie auch schon von betrügerischen

Kurznachrichten gehört. Hier geben sich Kriminelle oft als die Kinder oder Enkelkinder der Betroffenen aus und drängen auf eine Geldüberweisung.

Mit unserer Broschüre „Mehr Sicherheit“ möchten wir Ihnen eine ganz konkrete Hilfestellung an die Hand geben, die Sie im Alltag vor Betrügern und ihren Maschen schützt. Sie finden in diesem Heft erprobte Tipps und praktische Checklisten. Und natürlich sind wir bei der Sparda-Bank Südwest auch stets von Mensch zu Mensch für Sie da. Sprechen Sie uns bei Fragen gern an. Gemeinsam machen wir Ihre finanziellen Angelegenheiten noch sicherer.

**Inhalt**

<b>Statistik</b> Betrugsfälle nehmen zu	3	<b>Im Internet</b> Fake Shops und Co einfach erkennen	6	<b>Unsere Tipps</b> Diese Regeln gelten immer	9
<b>Am Telefon und Smartphone</b> Lassen Sie sich nicht unter Druck setzen!	4	<b>An der Haustür</b> So bleiben Betrüger draußen	8	<b>Unser Online-Banking</b> Bankgeschäfte sicher erledigen	10

Herausgeber: Sparda-Bank Südwest eG, Robert-Koch-Str. 45, 55129 Mainz-Hechtsheim, www.sparda-sw.de  
Stand: 01.08.2024. Die Informationen in diesem Magazin wurden mit größtmöglicher Sorgfalt zusammengestellt; für die dauerhafte Richtigkeit kann jedoch keine Gewähr übernommen werden. Bei direkten oder indirekten Verweisen auf fremde Internetseiten macht sich die Sparda-Bank Südwest eG deren Inhalt nicht zu eigen. Die Sparda-Bank Südwest eG haftet für die Inhalte dieser Internetseiten nicht. Die Verantwortlichkeit liegt allein beim jeweiligen Anbieter.

# Betrugsfälle nehmen zu

Kriminelle Betrüger nutzen ganz unterschiedliche Maschen, um ihre Opfer zu täuschen – und haben damit oft Erfolg, wie etwa das „Bundeslagebild Cybercrime“ für das Jahr 2023 des Bundeskriminalamts zeigt. Umso wichtiger ist es, sich jetzt zu schützen.

**Cybercrime: Datenklau steigt kräftig**

Für das Jahr 2023 verzeichnet etwa die rheinland-pfälzische Polizei im Bereich Cyberkriminalität einen Anstieg von fast **20 Prozent** im Vergleich zum Vorjahr. Dabei geht es um Delikte wie Computersabotage, Ausspähen oder das Abfangen von Daten.



**Immer mehr Schockanrufe**

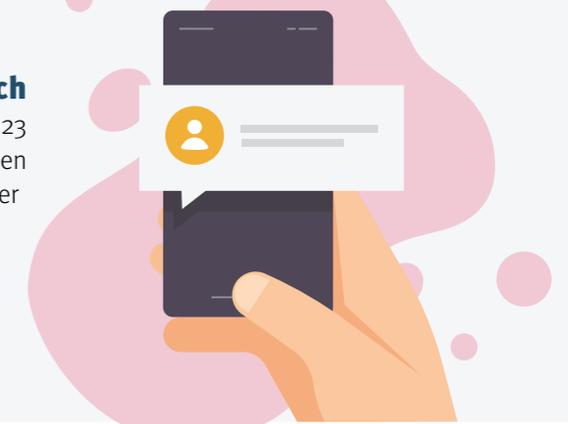
Die Zahl der Schockanrufe hat in Rheinland-Pfalz zugenommen. 2023 hat es laut Landeskriminalamt 12.958 Fälle in diesem Bereich gegeben. Bei sogenannten Enkeltrick-Anrufen gab es einen Anstieg von 19 Prozent, bei Anrufen von angeblichen Amtsträgern sogar von 28 Prozent. Für Betroffene ist so ein Schaden in Höhe von rund **10,6 Mio. Euro** entstanden.



**22.000**  
**Beschwerden**

**SMS-Betrug häuft sich**

Bei der Bundesnetzagentur gingen allein im Jahr 2023 bis Mai rund **22.000 Beschwerden** ein, bei denen es um Betrugsversuche per SMS ging. 14.000 dieser Beschwerden betrafen den Enkeltrick.



Bilder: iStock (rambot82, YoGinta, Elena Lukanova [2], cttlaplus), Andreea Schombara; Titel: iStock (Whiskerz)

# 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!



## 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 Datenschutzcheck und legen Ihre Einstellungen fest.

**G**ehört haben Sie bestimmt schon mal von diesen Betrugsvarianten: Einzeltrick, falsche Polizisten am Telefon, 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 können, denken Sie immer daran:

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

19:30

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 also nicht und legen Sie einfach auf. Dann können Sie einmal tief durchatmen und anschließend die 110 wählen, um der Polizei den Sachverhalt zu schildern. ●



## 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.

## 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 sich den Sachverhalt bestätigen lassen.



## WhatsApp-Nachrichten: Vorsicht bei unbekannt 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 unbekannt

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, machen Sie Screenshots und melden Sie den Vorfall der Polizei. Löschen Sie dann den Chat.

## Checkliste Chatbetrug

- **Keine unbekannt Nummer aufnehmen** in die WhatsApp-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.



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

Immer wieder geben sich Betrüger am Telefon als Mitarbeiter Ihrer Sparda-Bank oder eines anderen Instituts aus. Nicht selten erscheint im Display sogar die korrekte Rufnummer. Das Ziel der Kriminellen: Sie dazu zu bringen, eine Transaktion mit Ihrer Freigabe-App zu

bestätigen. Kein echter Bankmitarbeiter würde Sie je dazu auffordern!

### 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 „Mitarbeiter“

- **Das Gespräch sofort beenden.** Kein echter Bankmitarbeiter drängt je zur Freigabe von Transaktionen oder zur „Bestätigung“ von Daten.
- **Keine Fremdprogramme installieren** auf Ihrem PC, Tablet oder Smartphone.
- **Nicht auf Drohungen reagieren**, wenn etwa ein falscher Mitarbeiter behauptet, Ihre Konten würden gesperrt.



Bilder: iStock (rambo82, Robert Aneszko, Milian Markovic)

## Fake Shops und Co einfach erkennen



### 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 [www.verbraucherzentrale.de/fakeshopfinder](http://www.verbraucherzentrale.de/fakeshopfinder)



Echt aussehende E-Mails oder Online-Shops: Internetbetrüger legen sich ins Zeug, um Sie zu täuschen. Wir erklären, wie Sie Kriminellen nicht ins Netz gehen.

Die digitale Welt ermöglicht es Betrügern, mit immer neuen Tricks an die Daten ihrer Opfer zu gelangen. Täuschend echt aussehende E-Mails oder seriös auftretende Online-Shops verleiten dazu, auf Links zu klicken oder ein vermeintliches Superschnäppchen in den Warenkorb zu legen und sensible Bankdaten preiszugeben. Doch Transaktionen in solchen sogenannten Fake Shops lassen sich nur schwer zurückbuchen. Sollten Betrüger Ihre Bank- oder Kreditkartendaten haben, müssen Sie Ihren Online-Banking-Zugang bzw. die Kreditkarte sofort sperren lassen! Mit

aufmerksamem Verhalten im digitalen Alltag können Sie sich aber grundsätzlich vor Fake Shops und Co schützen (siehe rechts).

### Doppelt gesichert hält besser

Führen Sie Online-Einkäufe und Online-Banking-Aufträge am besten nur mit der sogenannten Zwei-Faktor-Authentifizierung durch. Dieses Schutzverfahren bestätigt Ihre Identität aus zwei unterschiedlichen Quellen. So können Sie sich vor Fremdzugriffen auf Nutzerkonten und Identitätsdiebstahl schützen.



### Achtung, Fake Shop: 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. Dann ist Ihr Geld weg und die 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 bei den bekannten Vergleichsportalen

#### 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.** Nutzen Sie dafür

den **Fake-Shop-Finder der Verbraucherzentrale!** Suchen Sie außerdem 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.

höher, spricht das fast immer für Betrug.



### Vorsicht, Phishing: So gehen Sie Datendieben nicht an den Haken

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

#### Webadresse auf Echtheit prüfen

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

#### Checkliste Phishing

- **Löschen Sie E-Mails,** wenn Sie darin zur Eingabe von persönlichen Daten wie Passwörtern oder Kundendaten aufgefordert werden.
- **Klicken Sie nicht auf Links,** die in Nachrichten von Banken oder Unternehmen (z. B. eBay) 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.
- **Geben Sie immer die URL der Website in die Adresszeile im Browser ein,** um sicherzustellen, dass Sie die echte Website aufrufen.

Schlosssymbol können Sie die Echtheit prüfen.

# So bleiben Betrüger draußen

Kriminelle nutzen viele Tricks, um sich Zutritt zu Ihren Wohnräumen zu verschaffen. Wir zeigen, wie Sie sich davor schützen können.



Bilder: iStock (sturti, rambot& [2], FANDSrabutam)

**D**er direkte Zugang zu Ihrem Haus oder Ihrer Wohnung ist für Betrüger wie ein Sechser im Lotto. Seien Sie daher unbedingt skeptisch, wenn unangekündigt vermeintliche Polizisten vor der Tür stehen und Sie über angebliche Einbrüche in der Gegend informieren wollen. Spätes-

tens bei der Frage nach Wertgegenständen in Ihrem Zuhause sollten die Alarmglocken klingeln. Das gilt auch, wenn vermeintliche Mitarbeiter von Gas-, Wasser- oder Stromwerken unter einem Vorwand zu Ihnen wollen. Hier sollte Ihre Tür einfach geschlossen bleiben.



## Seien Sie bitte misstrauisch!

Klingelt es unangekündigt an Ihrer Haustür, heißt es lieber erst einmal Vorsicht! Legen Sie die Türkette an und öffnen Sie die Tür nur einen Spalt oder sprechen Sie durch die geschlossene Tür. Reagieren Sie auch bei angeblichen Notfällen wie einem Gasleck oder Wasserrohrbruch überlegt – das heißt: Erkundigen Sie sich in aller Ruhe telefonisch beim Hausmeister, bei den Nachbarn oder direkt bei den Stadtwerken, ob überhaupt ein Notfall vorliegt. Vorsicht ist auch angebracht, wenn jemand um ein Glas Wasser bittet oder einen Zettel für den Nachbarn abgeben

### Checkliste **Haustür**

- **Prüfen Sie, wer vor der Tür steht:** Öffnen Sie nicht für Unbekannte und übergeben Sie niemals Wertsachen an „Polizisten“.
- **Ausweis zeigen lassen:** Verlangen Sie danach, den Dienstaussweis zu sehen, und schauen Sie genau hin.
- **Nur nach Terminvereinbarung öffnen:** Lassen Sie nur Personen rein, die sich vorher per Termin angekündigt haben.
- **Nachbarn um Hilfe bitten:** Ziehen Sie eine Vertrauensperson hinzu, wenn Sie Zweifel haben.

möchte. Auch hier gilt: Lassen Sie niemand Fremdes in die Wohnung!

# 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 beim Anruf von Fremden! Sagen Sie, dass es gerade ungünstig ist, und bieten Sie einen Rückruf an. Reagiert der Anrufende darauf 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.



### Infos vom Landeskriminalamt

Viele Täter bzw. Tätergruppen versuchen gezielt, ältere Menschen durch Betrug an der Haustür, am Telefon oder im Internet um ihr Hab und Gut zu bringen. Tipps, wie sich Seniorinnen und Senioren davor schützen können, gibt z. B. das Landeskriminalamt Saarland.



## 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. Betrüger können auch unter Ihnen bekannten Telefonnummern anrufen. Seien Sie wachsam!

## 4. Den Dienstaussweis zeigen lassen

Wenn Unbekannte vor Ihrer Haustür stehen und sich als Polizisten oder andere Amtspersonen ausgeben, dann gilt: Lassen Sie sich unbedingt den Dienstaussweis zeigen und lassen Sie Fremde auf keinen Fall in Ihr Haus oder Ihre Wohnung!

## 5. 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.

## 6. Niemals Log-in-Daten preisgeben

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



# Bankgeschäfte sicher erledigen!

Wir bieten modernes Online-Banking mit höchsten Sicherheitsstandards. Sie selbst können mit weiteren Schutzmaßnahmen für noch mehr Sicherheit sorgen.

**E**ine Sache ist klar: Mit dem Online-Banking der Sparda-Bank Südwest erledigen Sie Ihre Bankgeschäfte jederzeit sicher und sorgenfrei. So können Sie zum Beispiel mit der App SpardaSecureGo+ Ihre Online-Banking-Transaktionen wie Überweisungen, Serviceaufträge oder Daueraufträge schnell und sicher per App auf Ihrem Smartphone bestätigen. Doch auch wenn die Technik reibungslos funktioniert, sollten Sie auf jeden Fall weitere Schutzmaßnahmen beachten, um sich vor Betrugsmaschen zu schützen, mit denen Kriminelle auf Ihre sensiblen Daten zugreifen wollen.

## Echtheit der Website überprüfen

Wir setzen auf modernste Sicherheitstechniken und tun alles, um Ihnen bestmöglichen Schutz beim Online-Banking zu bieten. Und auch Sie selbst können dazu beitragen. Um unsere Website aufzurufen und sich im Online-Banking anzumelden, geben Sie am besten immer die URL [www.sparda-sw.de](http://www.sparda-sw.de) in die Adresszeile des Browsers ein, um sicherzustellen, dass Sie die echte Website der Sparda-Bank Südwest aufrufen. Speichern Sie außerdem nie Zugangsdaten im Browser oder auf dem PC! Unsere Empfehlung: Die Nutzung der SpardaBanking App zusammen mit der App SpardaSecureGo+ bietet ein hohes Maß an Sicherheit für alle Transaktionen.

## Transaktionsdaten genau prüfen

Mit der App SpardaSecureGo+ und dem „Sm@rt-TAN plus“-Verfahren bieten wir Ihnen

zwei sichere Möglichkeiten, Ihre Bankaufträge freizugeben. Ganz wichtig: Prüfen Sie vor jeder Freigabe genau, ob die Transaktionsdaten mit dem von Ihnen im Online-Banking veranlassenden Auftrag übereinstimmen. Da stimmt etwas nicht? Dann geben Sie die Transaktion auf keinen Fall frei und informieren Sie uns bitte umgehend!

## Überprüfen Sie E-Mail-Absender genau!

Ganz wichtig: Ihre Sparda-Bank fordert Sie niemals per Anschreiben oder E-Mail dazu auf, vertrauliche Daten wie Sparda-NetKey, Alias, PIN oder TAN anzugeben! Öffnen Sie daher bitte auch niemals einen Link in einer E-Mail, wenn Sie den Absender nicht kennen. Fragen Sie im Zweifel immer lieber bei uns nach! Nutzen Sie für eine sichere Kommunikation die Nachrichtenfunktion im Online-Banking oder in der Banking-App.

## Lieber sicher bezahlen

Bezahlen Sie Ihre Online-Einkäufe am besten bequem und sicher mit Ihrer Mastercard® und dem Bezahlfahrer Mastercard Identity Check. Oder nutzen Sie eine klassische Überweisung im Online-Banking. Und denken Sie dran: Überprüfen Sie vor der Bezahlung die Echtheit des Online-Shops – zum Beispiel mit dem Fake-Shop-Finder der Verbraucherzentrale (siehe Seite 6 und 7).

## Aktuelle Sicherheitshinweise beachten

### Bleiben Sie auf dem Laufenden:

Online-Betrüger lassen sich immer wieder neue Maschen und Tricks einfallen, um an Ihre sensiblen Daten zu kommen.

### Geben Sie den Betrüger keine Chance

und informieren Sie sich regelmäßig über die aktuellsten Betrugsversuche. Schauen Sie am

besten auf unserer Internetseite (siehe unten) mit den aktuellen Sicherheitshinweisen vorbei.

### Und wenn Sie doch versehentlich reagiert haben?

Dann sperren Sie Ihren Online-Banking-Zugang und nehmen bitte unverzüglich Kontakt zu uns auf unter **0 61 31 63 63 63**.

[www.sparda-sw.de/sicherheit](http://www.sparda-sw.de/sicherheit)



## Noch sicherer unterwegs mit SpardaSurfSafe

SpardaSurfSafe bietet Schülerinnen und Schülern in unserem Geschäftsbereich Hintergrundwissen zu aktuellen Themen rund ums Netz. Zum Angebot gehören auch spannende Live-Events. Plus: Jeden Donnerstag können Kids im Live-Chat Fragen stellen! Mehr unter [www.sparda-sw-stiftung.de/surfsafe](http://www.sparda-sw-stiftung.de/surfsafe)

## DEVK-Cyberversicherung: gut geschützt im Netz



**DEVK**

**Egal ob zu Hause am PC oder unterwegs am Smartphone** – ein großer Teil unseres Alltags findet mittlerweile online statt. Parallel dazu ist die Computerkriminalität zu einem großen Geschäft geworden. So versuchen es Internetbetrüger mithilfe von Phishing über E-Mails oder Trojaner immer wieder, an Ihre Bankdaten zu kommen.

**Die Cyberversicherung der DEVK schützt Sie** gegen die daraus entstehenden Vermögensschäden bis zu 10.000 Euro pro Jahr. Versichert sind der Missbrauch bei Verwendung von Bank-, Kredit- und sonstigen Debitkarten der Sparda-Bank Südwest sowie der Missbrauch Ihres Kontos und Ihres privaten Online-Bankings.

**Für nur 2,50 Euro pro Monat** sorgt die Versicherung bei Ihrem Online-Banking für ein besseres Gefühl. Sprechen Sie uns gern an. Weitere Infos unter [www.sparda-sw.de/cyberversicherung](http://www.sparda-sw.de/cyberversicherung)



**SICHER** online  
unterwegs

nur  
**2,50€**  
pro Monat

**Günstiger Schutz mit der  
Cyberversicherung –  
jetzt die ersten 6 Monate kostenfrei sichern**

- ✓ Schutz bis zu 10.000 Euro pro Jahr
- ✓ jährlich bis zu drei Schäden versichert
- ✓ Versicherungsschutz gilt weltweit

**DEVK**

[www.sparda-sw.de/cyberversicherung](http://www.sparda-sw.de/cyberversicherung)

**Sparda-Bank**