Mehr Sicherheit

Lassen Sie sich nicht ködern! Im Internet, am Telefon oder an der Haustür: die besten Tipps gegen Trickbetrug.

Sparda-Bank

Die Deine Bank.

*„Legen Sie die **Grundregeln** für den Fall der Fälle griffbereit neben Ihr Telefon.“*

Sie haben vielleicht auch schon in Ihrem Bekannten- und Freundeskreis davon gehört. Von der WhatsApp-Nachricht der angeblichen Tochter, die eine neue Handynummer habe und plötzlich Geld brauche. Vom vermeintlichen Online-Schnäppchen in einem sogenannten Fake Shop, das nach der Bestellung nie versendet wurde. Von der E-Mail, in der dazu aufgefordert wird, sich mit seinen persönlichen Bankdaten neu zu identifizieren. Die Liste der Vorgehensweisen bei solchen kriminellen Betrugsversuchen ist lang und es kommen immer neue hinzu.

Umso mehr freut es mich, dass wir Ihnen mit unserer neuen Sicherheitsbroschüre im Detail und mit kompakten Checklisten aufzeigen können, wie Sie sich vor Betrügern und ihren zahlreichen Maschen schützen können.

Meine persönliche Empfehlung: Trennen Sie die Seite 9 aus der Broschüre heraus und legen Sie diese Grundregeln griffbereit neben Ihr Telefon. So haben Sie im Fall der Fälle immer die wichtigsten Leitlinien parat, wie Sie sich bei einem Betrugsversuch konkret verhalten sollten.

Hermann-Josef Simonis,
Vorstand der Sparda-Bank West

Inhalt

Statistik

Betrugsfälle nehmen zu

Kriminelle Betrüger entwickeln immer neue Maschen, um ihre Opfer zu täuschen – und haben damit oft Erfolg, wie etwa die aktuelle Statistik des Bundeslagebilds Cybercrime von August 2023 zeigt. Umso wichtiger ist es, sich jetzt zu schützen.

Cybercrime: Datenklau steigt kräftig

Für 2022 registrierte die polizeiliche Kriminalstatistik **136.865 Straftaten** im Bereich Cybercrime. Das sind rund 11 Prozent mehr als 2019. Vor allem beim Ausspähen und Abfangen von Daten gab es 2022 einen deutlichen Anstieg von Straftaten. Gegenüber 2019 stiegen sie sogar um 33 Prozent.

+33 %

Immer mehr Schockanrufe

Die Zahl der Schockanrufe hat in Nordrhein-Westfalen im letzten Jahr deutlich zugenommen: 2022 wurden dem Landeskriminalamt **8.210 Fälle** gemeldet. 2021 waren es landesweit noch 6.919 Betrugsfälle. Das entspricht einem Anstieg von mehr als 15 Prozent.

+15 %

Messenger-Betrug häuft sich

Das Bundeskriminalamt registrierte allein in den ersten acht Monaten des Jahres 2022 rund **40.000 Fälle** von Messenger-Betrug. Der Gesamtschaden belief sich auf rund 22 Millionen Euro.

22 Mio. EUR

WhatsApp-Tipp

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

Am Telefon und Smartphone

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, 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: 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 unbekannten Nummern

An den Austausch von Nachrichten mit Freunden oder der Familie über Messenger-Programme 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 unbekannten Rufnummer erscheint. Folgt dann kurz darauf noch die Bitte, Geld für einen Notfall zu überweisen, sollten Sie alarmiert sein.

Der Rat der Polizei:
Löschen Sie solche Nachrichten sofort! Antworten Sie auf keinen Fall und speichern Sie die Nummer nicht.

Checkliste **Chatbetrug**

- **Keine unbekannte 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.

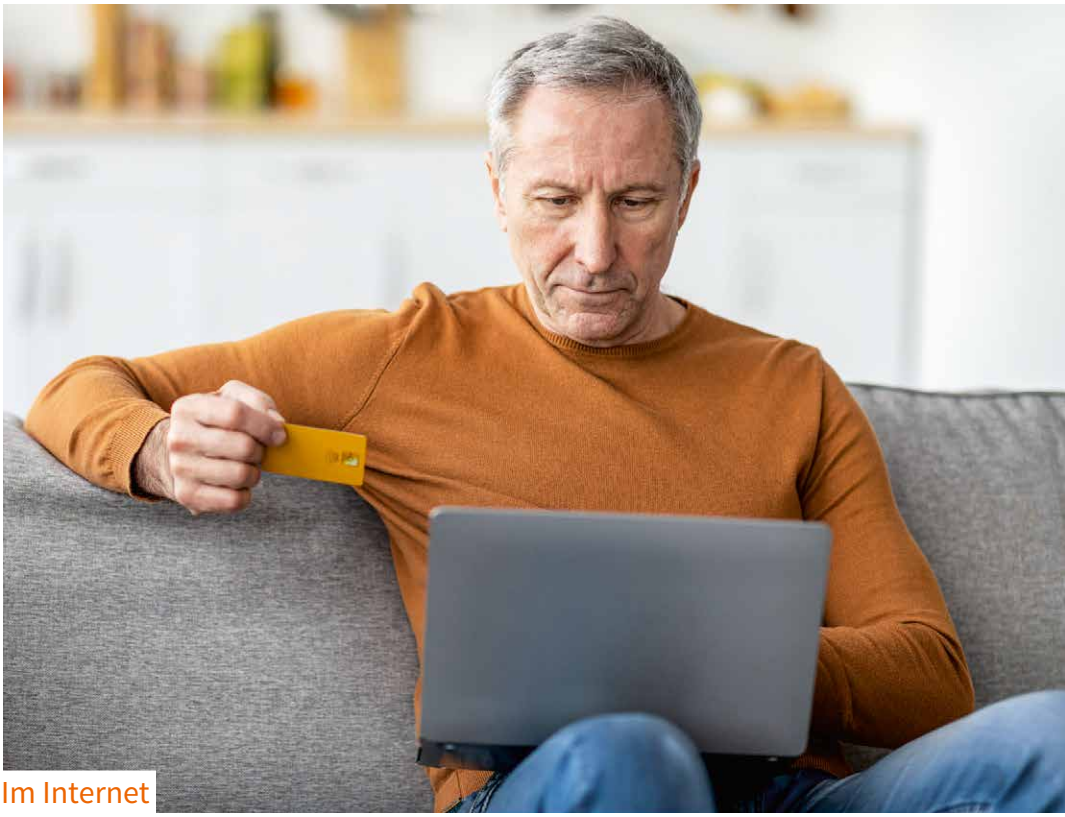
Falscher Mitarbeiter am Telefon: Auflegen ist die richtige Wahl

„Sie haben die neueste Windows-Version noch nicht installiert? Dann helfe ich Ihnen gern weiter.“ So oder ähnlich melden sich immer wieder angebliche Microsoft-Mitarbeiter am Telefon. Doch dieses Serviceangebot hat immer das gleiche Ziel: Zugriff auf Ihren Computer zu bekommen, um Daten wie 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 **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 der Mitarbeiter behauptet, dass Ihre Windows-Version gelöscht wird.



Im Internet

Fake Shops und Co einfach erkennen

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.

Diese Sperrnummern sollten Sie sich notieren!

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

BankCard (Debitkarte)
116 116 (kostenfrei)

Mastercard®
(Kreditkarte)
0 69 66 57 17 72

Sperrung des Online-Bankings
0211 23 93 23 93
(24 Stunden/7 Tage)

Tipp: Einfach QR-Code scannen und wichtige Sperrnummer im Handy einspeichern!

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.nrw/fakeshopfinder

Achtung, Fake Shop: So shoppen Sie sicher im Internet

Egal ob Markenkleidung, Fotoausrüstung, Smartphone oder Parfüm: Die Versuchung, sich auf der Shopping-Tour 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 deutlich höher, spricht das fast immer für Betrug.

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 „Vorauskasse“ oder „Sofortüberweisung“.** Es sollte auch andere Zahlungsmöglichkeiten geben. Auch eine Widerrufsbelehrung muss da sein.

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 West 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 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.

Checkliste **Phishing**

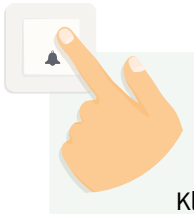
- **Löschen Sie E-Mails,** wenn Sie darin zur Eingabe von persönlichen Daten wie Passwörtern oder Kundendaten aufgefordert werden.
- **Klicken Sie nicht auf Links,** die in Nachrichten von Banken oder Unternehmen enthalten sind. Melden Sie sich direkt in Ihrem Nutzerkonto an und prüfen Sie dort, ob es 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.

An der Haustür

So bleiben Betrüger draußen

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

Der 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. Spätestens bei der Frage nach Wertgegenständen in Ihrem Zuhause sollten die Alarmglocken klingeln. Das gilt auch, wenn vermeintliche Mitarbeitende 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 Türsperre 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 – d. h.: 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 möchte. Auch hier gilt: Lassen Sie niemand Fremdes in die Wohnung!

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 Dienstausweis 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.

Unsere Tipps

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 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.

4. Den Dienstausweis zeigen lassen

Wenn Unbekannte vor Ihrer Haustür stehen und sich als Polizisten oder andere Amtspersonen ausgeben, dann gilt: Lassen Sie sich unbedingt den Dienstausweis 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.

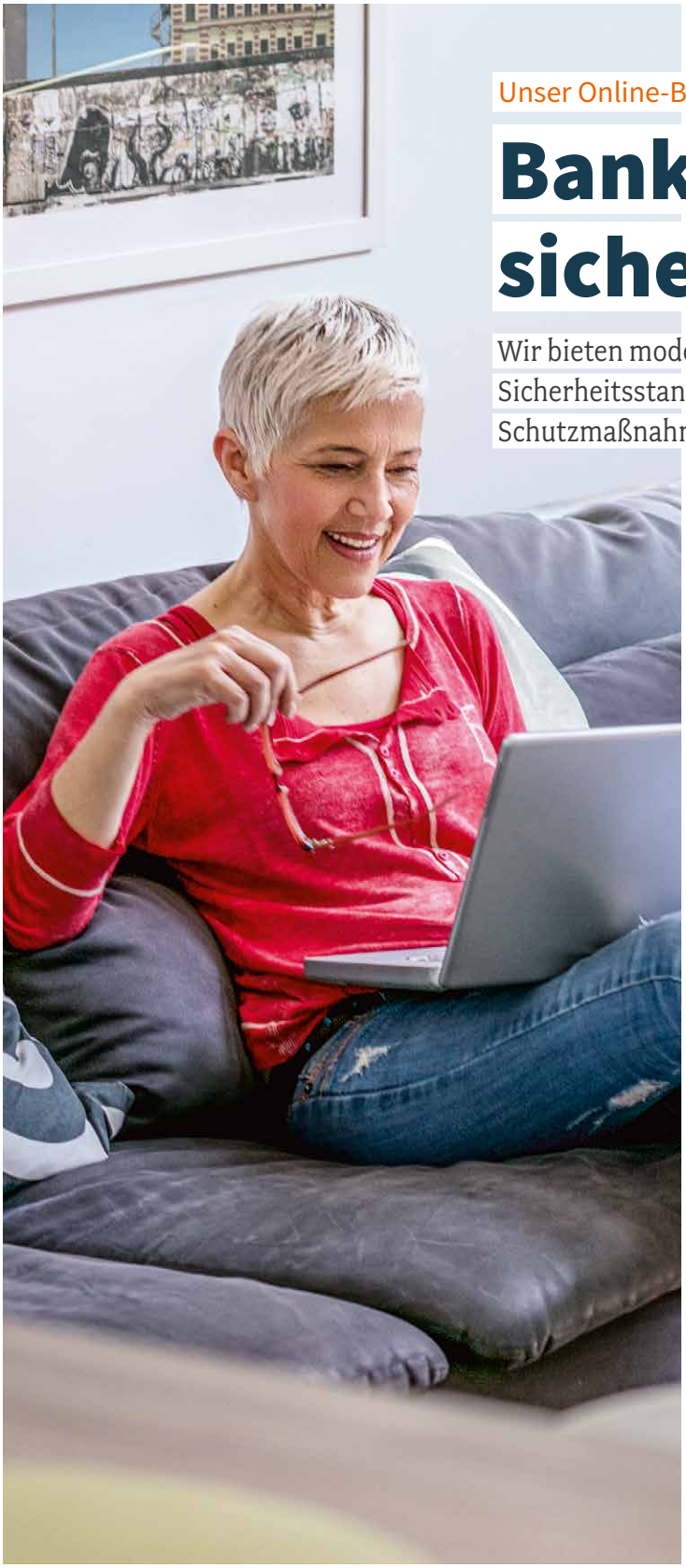
6. Niemals Log-in-Daten rausgeben

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

Infos vom LKA

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 das Landeskriminalamt (LKA) Nordrhein-Westfalen unter

lka.polizei.nrw/senioren



Fotos: AdobeStock/Song_about_summer, iStock/Nikola Ilic; Illustrationen: Adobe Stock/ buravleva_stock, HMC

Unser Online-Banking

Bankgeschäfte sicher erledigen!

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

Eine Sache ist sicher: Mit dem Online-Banking der Sparda-Bank West erledigen Sie Ihre Bankgeschäfte jederzeit sicher und sorgenfrei. So können Sie zum Beispiel mit der SpardaSecureApp ohne TAN-Eingabe 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.

Immer verschlüsselt kommunizieren

Erledigen Sie Ihre Online-Bankgeschäfte immer über das geschützte sogenannte https-Protokoll. Achten Sie darauf, dass die Internetadresse (URL) mit **https://** beginnt. Zusätzlich können Sie mit einem Klick auf das kleine Schloss links neben der URL und dem angezeigten Zertifikat die Echtheit der Website prüfen. Zudem bietet die Nutzung der SpardaApp zusammen mit der SpardaSecureApp ein hohes Maß an Sicherheit für alle Transaktionen.

Nicht auf unbekannte E-Mails reagieren

Ganz wichtig: Ihre Sparda-Bank fordert Sie niemals per Anschreiben oder E-Mail dazu auf, vertrauliche Daten wie PIN, TAN

oder Kontonummern 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!

Lieber sicher überweisen
Bezahlen Sie Ihre Online-Einkäufe am besten per Überweisung im Online-Banking oder der SpardaApp. Verzichten Sie auf eine Sofortüberweisung mit Zahlungsdienstleistern wie Klarna & Co. Sonst ist im Betrugsfall – etwa wenn die Ware nicht kommt – keine Wiederbeschaffung möglich.

Das Plus an Sicherheit für Ihr Online-Konto
Greifen Dritte doch einmal ohne Ihr Verschulden auf Ihr Online-Konto zu, übernimmt Ihre Sparda-Bank die Haftung. Dann greift die SicherheitsPlus-Garantie. Wir haften bei Schäden durch missbräuchliche Verwendung Ihrer Zugangsdaten, sofern nicht Ihr eigener Pflichtverstoß die Ursache war. So wird Ihr Online-Banking bei der Sparda-Bank West erst recht zu einer sicheren Sache.

Mit Sicherheit gut beraten!

Sie sind sich noch unsicher, ob eine Cyberversicherung für Sie sinnvoll ist? Gern zeigen wir Ihnen in einem Beratungsgespräch, welchen Versicherungsschutz Sie benötigen. Vereinbaren Sie einfach einen Termin telefonisch unter

0211 23 93 23 93,

im Internet unter

www.sparda-west.de/termin

oder über Ihr Online-Banking und die Sparda-App.

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 Betrügern 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 **0211 23 93 23 88!**

www.sparda-west.de/sicherheitshinweise

DEVK Cyberversicherung: Gut geschützt im Netz

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 West 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 erhalten Sie auch unter **www.sparda-west.de/cyberversicherung**

DEVK

Partner der Sparda-Bank

Online-Banking ohne Sorgen.

Die DEVK Cyberversicherung:

Ihr günstiger Schutz gegen Cybercrime.

Wer die Weiten des Cyberspace unvorbereitet betritt, läuft Gefahr, sich darin zu verlieren. Denn mit der Digitalisierung entstand ein Raum, den sich auch Online-Betrüger zunutze machen. Bewegen Sie sich ab sofort sicher im World Wide Web und setzen Sie auf den günstigen Schutz der DEVK Cyberversicherung.

Mehr erfahren unter
www.sparda-west.de/
cyberversicherung

Sparda-Bank

Die Deine Bank.