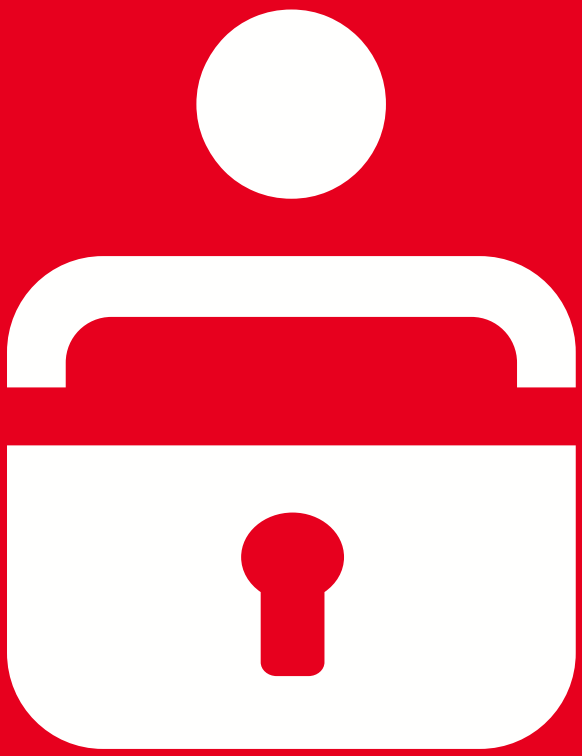
Gelassen ist einfach.

Wenn Sie Ihre Finanzgeschäfte und Online-Einkäufe jederzeit und überall sicher erledigen können.

Wenn’s um Geld geht



Online einkaufen und Finanzgeschäfte erledigen? Nichts einfacher als das. Und die Sicherheit? Darum kümmern wir uns. Auf unser Online-Banking und unsere Online-Bezahlverfahren können Sie sich sicher verlassen.

Online-Banking
Ihre Vorteile 4
Was Sie brauchen 5
Sicherungsverfahren 6
Anmelden 8
Überweisen 9
Sicherheitstipps 11

paydirekt
Sicher online bezahlen 12
Registrieren und bezahlen 13

Mit Kreditkarte online bezahlen
Registrieren 14
Zahlen – Schritt für Schritt 15
Sicherheitstipps 16

Sicherheit im Internet 17

Was tun im Notfall? 20

Schnell, einfach, bequem und sicher

Unser Alltag ist hektisch, schnelllebig und nicht immer einfach. Damit Sie mehr Zeit für die wesentlichen Dinge im Leben haben, bieten wir ein sicheres Online-Banking. Das können Sie erwarten:

Schnell erledigt
Mit wenigen Klicks: Überweisungen tätigen, Daueraufträge einrichten und Kontoauszüge prüfen. So sparen Sie viel Zeit.

Einfach erledigt
Die intuitive Bedienbarkeit des Online-Bankings und eine übersichtliche Gestaltung helfen Ihnen, sich zurechtzufinden.

Bequem erledigt
Sie haben überall Zugriff auf Ihre Konten und vor allem immer dann, wenn Sie Zeit haben.

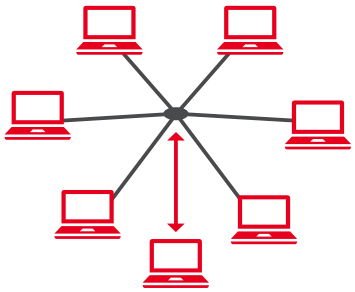
Sicher erledigt
Das Online-Banking Ihrer Sparkasse arbeitet mit höchsten Sicherheitsstandards, sodass Ihr Geld optimal geschützt ist.

Die Basis für Online-Banking

Sparkassen-Konto
Ihr erster Schritt zum Online-Banking ist die Eröffnung eines Kontos. Sollten Sie bereits Kunde bei uns sein, können Sie Ihr Online-Banking jederzeit kostenlos freischalten lassen. Mit der Multibanking-Funktion haben Sie zudem die Möglichkeit, Ihre Konten und Depots anderer Finanzinstitute direkt im Online-Banking Ihrer Sparkasse zu managen.

Computer, Smartphone oder Tablet
Für das Online-Banking brauchen Sie vor allem einen Computer oder ein anderes internetfähiges Endgerät, wie etwa ein Smartphone oder ein Tablet. Speziell für die Nutzung auf mobilen Endgeräten ist die Sparkassen-App gedacht.

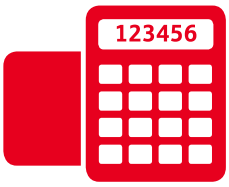
Internetzugang
Um das Online-Banking nutzen zu können, muss Ihr Endgerät über eine Verbindung mit dem Internet verfügen. Dabei kommt es nicht auf die Geschwindigkeit an: Das Sparkassen-Online-Banking funktioniert – egal, ob Sie über ein Highspeed-Kabelnetz oder mit Ihrem Smartphone surfen.



Sicherheit
Nicht nur für das Online-Banking ist die Installation eines aktuellen Internetbrowsers bzw. einer speziellen Bankensoftware, eines Virenschutzprogramms und einer „Firewall“ dringend zu empfehlen. Um Transaktionen durchzuführen, benötigen Sie für einige Sicherungsverfahren zusätzlich ein spezielles Kartenlesegerät. Mehr dazu erfahren Sie auf den nächsten Seiten.

Für Ihre Sicherheit

Unsere Sicherheitssysteme sind immer auf dem neuesten Stand und bieten Ihnen ein Höchstmaß an Schutz: Eine Anmeldung im Online-Banking funktioniert ausschließlich mit Ihrem persönlichen Anmeldenamen und der dazugehörigen PIN.* Für jede Ihrer Transaktionen benötigen Sie eine separate Transaktionsnummer (TAN), mit der Sie beispielsweise Ihre Überweisungen freigeben oder sich regelmäßig im Online-Banking authentifizieren. Es stehen Ihnen unterschiedliche Sicherungsverfahren zur Verfügung – fragen Sie Ihre Sparkasse, welche der TAN-Verfahren sie anbietet.



chipTAN – sicher mit Debitkarte und TAN-Generator
Mithilfe eines TAN-Generators und Ihrer Sparkassen-Card (Debitkarte) erzeugen Sie selbst Ihre TAN. Der TAN-Generator ist ein kleines, kabelloses Gerät, ähnlich einem Taschenrechner. Sie erhalten ihn direkt von uns oder bestellen ihn online in unserem Sparkassen-Shop.

Die Vorteile von chipTAN:

- → Kontrollmöglichkeit durch Anzeige der wichtigsten Auftragsdaten.
- → Sicherheitsrelevante Informationen befinden sich nur auf Ihrer Sparkassen-Card (Debitkarte).
- → Kein Missbrauch möglich, da jede erzeugte chipTAN nur für einen bestimmten Auftrag gültig ist.
- → Wenn Sie Ihren TAN-Generator dabeihaben, können Sie auch von jedem anderen Endgerät (Computer, Tablet oder Smartphone) Aufträge ausführen.

* Zum Log-in ins Online-Banking geben Sie spätestens nach 90 Tagen wieder eine TAN ein.

pushTAN – für alle, die viel unterwegs sind
Ihre TAN erhalten Sie über die S-pushTAN-App direkt auf Ihr Smartphone oder Tablet. So können Sie ganz leicht mobil Ihre Finanzgeschäfte erledigen – ohne weitere Zusatzgeräte. Auf mobilen Endgeräten mit verändertem Betriebssystem, z. B. durch Jailbreak oder Rooten, wird die Nutzung der pushTAN-App unterbunden.

Die Vorteile der pushTAN:

- → Jede pushTAN ist zeitlich begrenzt und gilt nur für einen bestimmten Auftrag.
- → Empfang überall und jederzeit auf Ihr Smartphone oder Tablet (Datenverbindung vorausgesetzt).
- → Kontrollmöglichkeit durch Anzeige der wichtigsten Auftragsdaten.
- → Es ist kein zweites mobiles Endgerät notwendig: Die pushTAN erhalten Sie auf demselben Gerät, auf dem Sie mobil Ihre Finanzgeschäfte erledigen.

Ihr Einstieg: die Erstanmeldung

Mit Ihrer Freischaltung zum Online-Banking erhalten Sie von uns entweder eine Legitimations-ID oder Ihren persönlichen Anmeldenamen sowie eine Start-PIN. Mit diesen Zugangsdaten können Sie sich zum ersten Mal im Online-Banking anmelden. Und so geht's:

1. Stellen Sie die Verbindung zum Internet sicher und rufen Sie über einen Internetbrowser unsere Internetseite auf.

2. Über die Startseite können Sie sich im Online-Banking anmelden.

3. Tragen Sie nun Ihren erhaltenen Anmeldenamen bzw. Ihre Legitimations-ID in das Feld „Anmeldename“ und Ihre Start-PIN in das Feld „PIN“ ein.

4. Klicken Sie auf „Anmelden“.

5. Eventuell müssen Sie sich für das TAN-Verfahren, das Sie nutzen möchten, erst freischalten lassen. Weitere Informationen dazu erhalten Sie bei Ihrer Sparkasse.

6. Das System fordert Sie nun auf, eine persönliche, neue PIN einzugeben, die Sie selbst festlegen und mit einer TAN bestätigen. Die Start-PIN ist nur einmalig für den Erstzugang gültig. Außerdem können Sie einen individuellen Anmeldenamen hinterlegen, der Ihre automatisch vergebene Legitimations-ID bzw. den zuvor erhaltenen Anmeldenamen ersetzt. Zukünftig melden Sie sich somit immer mit Ihrem persönlich ausgewählten Anmeldenamen und der individuell festgelegten PIN in Ihrem Online-Banking an.

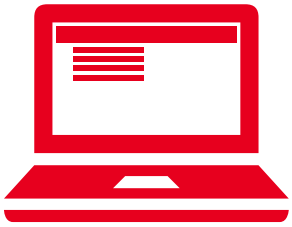
Wie überweise ich online?

1

Nachdem Sie sich mit Ihrem Anmeldenamen und Ihrer PIN über unsere Internetseite angemeldet haben, gelangen Sie zum Online-Banking.

Sie können jetzt sofort beginnen, Ihre Aufträge auszuführen, Daten zu ändern oder auch die aktuellsten Sicherheitstipps zu lesen. Eine der am häufigsten verwendeten Funktionen, die Überweisung, finden Sie hier erklärt.

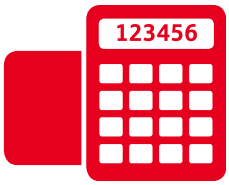
2



Klicken Sie in der oberen Menüleiste auf den Punkt „Online-Banking“ und dann auf „Banking“. Hier finden Sie die „Überweisung“. Mit dem angezeigten Überweisungsformular erstellen Sie Ihren Auftrag und senden diesen ab.

Der nächste Schritt unterscheidet sich, je nachdem welches Sicherungsverfahren Sie nutzen:

3



chipTAN
Auf dem Bildschirm erscheint nun eine sogenannte animierte Grafik in Form eines QR-Codes oder Flicker-Codes. Führen Sie Ihre Sparkassen-Card (Debitkarte) in den TAN-Generator ein und halten Sie diesen an die Position der animierten Grafik auf dem Bildschirm. Die Daten werden nun über die lichtempfindlichen Kontakte auf der Rückseite des TAN-Generators übertragen. Auf dessen Display werden die wichtigsten Daten Ihrer Überweisung angezeigt.

3 

pushTAN
Sie wechseln automatisch zur S-pushTAN-App und melden sich dort mit dem von Ihnen vergebenen Zugangspasswort an. Alternativ entsperren Sie die App mithilfe Ihres Fingerabdrucks (Touch-ID) oder durch Gesichtserkennung (Face-ID). Anschließend werden in der App die wichtigsten Daten Ihrer Überweisung angezeigt.

4 

Für beide Verfahren gilt: Prüfen Sie die Daten auf ihre Richtigkeit (bei einer Überweisung z. B. die letzten zehn Stellen der IBAN und den Betrag). Bei chipTAN: Bestätigen Sie mit der Taste „OK“ auf Ihrem TAN-Generator. Anschließend wird Ihnen die für diesen Auftrag generierte TAN angezeigt.

5 

Stimmen die Daten überein, können Sie den Auftrag am PC mit der übermittelten TAN freigeben. Fertig!

Finanzgeschäfte mobil erledigen
Mit der App **Sparkasse** können Sie Ihre aktuellen Kontostände einsehen und Überweisungen ausführen. Mit der Funktion „Fotoüberweisung“ geht’s noch schneller: Fotografieren Sie die jeweilige Rechnung – die zahlungsrelevanten Daten werden automatisch erkannt und in das Überweisungsformular übertragen. Zusätzlich können Sie sich in der Sparkassen-App zum nächstgelegenen Geldautomaten oder zur nächsten Sparkassen-Filiale lotsen lassen.

Mit Multibanking alle Konten im Griff
Führen Sie Konten oder Depots bei verschiedenen Finanzinstituten? In unserem Online-Banking und in der Sparkassen-App managen Sie sämtliche Ihrer Konten.
Im Online-Banking: In Ihrem Finanzstatus oder unter „Service“ und „Multibanking-Einstellungen“ fügen Sie beliebig viele Konten und Depots anderer Finanzinstitute hinzu und überblicken dort alle Ihre Kontostände.
In der Sparkassen-App: Unter „Finanzstatus“ und dann „Bearbeiten“ können Sie Ihre weiteren Konten und Depots eingeben. Nutzen Sie die App auch für Ihre Transaktionen von Konten und Depots anderer Finanzinstitute.

So geht sicheres Online-Banking

Wir tun viel für ein sicheres Online-Banking. Auch Sie können dazu beitragen, dass Ihre Daten sicher sind.

- **Vorsichtig sein:** Halten Sie Ihren Anmeldenamen und Ihre PIN geheim. Eine TAN geben Sie in der Regel nur ein, wenn Sie eine Transaktion ausführen möchten oder zur Authentifizierung im Online-Banking (alle 90 Tage). Denken Sie daran, wenn Sie nach diesen Daten gefragt werden.
  Tipp: Ändern Sie Ihre PIN in regelmäßigen Abständen, um unerlaubte Kontozugriffe zu erschweren.
- **Misstrauisch sein:** Wenn Ihnen etwas seltsam vorkommt, brechen Sie die Aktion lieber ab. Wir werden Sie niemals auffordern, eine TAN für Gewinnspiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen einzugeben.
- **Daten kontrollieren:** Auf dem Display Ihres TAN-Generators oder Ihres Mobiltelefons werden Ihnen die wichtigsten Auftragsdaten angezeigt. Falls die Daten nicht mit Ihrem Auftrag übereinstimmen, lieber abbrechen.
- **Sichere Eingabe:** Achten Sie bei der Anmeldung zum Online-Banking darauf, dass die Adresszeile in Ihrem Browser mit „https“ beginnt und das Schlosssymbol vorhanden ist. Melden Sie sich nach dem Online-Banking immer ab und löschen Sie den Cache Ihres Browsers.
- **Aufmerksam bleiben:** Kontrollieren Sie regelmäßig die Umsätze auf Ihrem Konto. Nur so erkennen Sie unberechtigte Abbuchungen rechtzeitig.
- **Tageslimit eingrenzen:** Legen Sie ein Tageslimit für Ihre Transaktionen im Online-Banking fest. Damit schränken Sie die Möglichkeiten unberechtigter Zugriffe ein.
- **Im Zweifel Zugang sperren:** Falls Sie den Verdacht haben, dass mit der Banking-Anwendung etwas nicht stimmt: Sperren Sie Ihren Zugang. Mehr Informationen hierzu finden Sie auf der Rückseite dieser Broschüre.

Bitte beachten Sie auch unsere allgemeinen Sicherheitstipps für das Internet auf Seite 19.

paydirekt – einfach und sicher online bezahlen

paydirekt ist das Online-Bezahlverfahren der deutschen Banken und Sparkassen. Damit bezahlen Sie gewohnt sicher, einfach und direkt mit Ihrem Sparkassen-Girokonto im Internet.

Ihre Vorteile: Bei Rückabwicklung einer Zahlung wird Ihnen das Geld direkt auf Ihr Girokonto gutgeschrieben. Sie können auf besonders hohe Sicherheitsstandards vertrauen, denn paydirekt nimmt auch beim Online-Bezahlen das Bankgeheimnis und den deutschen Datenschutz ernst. Ihre Daten werden nicht zu Werbezwecken an Dritte weitergegeben.

Mit paydirekt haben Sie alles im Griff:
Ihre Zahlungen können Sie immer in Ihrem Online-Banking, Ihrem Kundenbereich auf www.paydirekt.de oder mobil mit der paydirekt-App (bei Google Play und im App Store) prüfen. Dort verwalten Sie auch Ihre Anmeldedaten und vieles mehr.

Das besondere Sicherheits-Plus von paydirekt:
Während Sie zahlen, läuft eine Sicherheitsprüfung im Hintergrund. In Einzelfällen bestätigen Sie Ihre Zahlung, indem Sie zusätzlich eine TAN eingeben. Damit sind Sie bei paydirekt optimal abgesichert.

Käuferschutz inklusive
Sollte ein Händler einmal nicht liefern, erhalten Sie Ihr Geld zurück. Schnell und unkompliziert.

paydirekt

Für paydirekt registrieren und sicher bezahlen

Damit Sie schnell und einfach bezahlen können, schalten Sie sich am besten gleich für paydirekt frei:

1. Im Online-Banking Ihrer Sparkasse auf den Menüpunkt „paydirekt“ klicken.
2. Benutzername und Passwort vergeben und mit einer TAN bestätigen.
   Bei Bedarf sind wenige weitere Angaben nötig, z. B. zur Lieferadresse.
3. Link in der Aktivierungs-E-Mail bestätigen.

So zahlen Sie sicher in drei einfachen Schritten:

1. paydirekt im Online-Shop als Bezahlverfahren auswählen.
2. Name und Passwort eingeben.
3. Zahlung bestätigen – fertig.

Unter www.sparkasse.de/paydirekt erhalten Sie viele weitere Informationen. Zum Beispiel erfahren Sie dort, bei welchen Händlern Sie mit paydirekt bezahlen können.

Sicher ist sicher: Sollten Sie einmal nicht wissen, ob Sie eine Transaktion wirklich autorisiert haben, können Sie diese prüfen lassen. Hierfür klicken Sie in der Detailansicht im paydirekt-Käuferportal (www.paydirekt.de) auf „Problem melden“.

Mit Kreditkarte* online bezahlen

Beim Online-Shopping ist die Zahlung mit der Sparkassen-Kreditkarte eine beliebte Möglichkeit, schnell und sicher einzukaufen. In der Regel geben Sie für die Zahlung im Internet Ihre Kreditkartennummer, das Verfallsdatum Ihrer Kreditkarte und die Prüfziffer an.

mastercard ID Check

VISA SECURE

Einfach online bezahlen

Sie bezahlen gerne online mit Ihrer Kreditkarte? Dann beachten Sie jetzt: Online-Zahlungen mit Ihrer Kreditkarte sind in Kürze nur noch in Verbindung mit der S-ID-Check-App möglich. Laden Sie sich jetzt die S-ID-Check-App herunter und registrieren Sie Ihre Kreditkarte, damit Sie online bezahlen können.

Online sicher einkaufen mit dem S-ID-Check

Die S-ID-Check-App mit Mastercard® Identity Check™ oder Visa Secure bietet Ihnen höchste Sicherheit für Ihre Zahlungen mit der Kreditkarte im Internet. Sie bestätigen den Zahlbetrag Ihres Online-Einkaufs komfortabel mit der S-ID-Check-App.

Laden Sie jetzt die S-ID-Check-App herunter und registrieren Sie sich in der App.

Laden im App Store

JETZT BEI Google Play

Einfach QR-Code einscannen und App gleich herunterladen.

Und so geht's:

- → Laden Sie die S-ID-Check-App herunter.
- → Registrieren Sie sich in der S-ID-Check-App.
- → Ihre Identität bestätigen Sie entweder sofort über Ihr Online-Banking oder Sie fordern einen Aktivierungscode zur Freischaltung an.
- → Bei Händlern, die am Sicherheitsverfahren Mastercard® Identity Check™ oder Visa Secure teilnehmen, bestätigen Sie den Zahlbetrag Ihres Online-Einkaufs mit Ihrer Kreditkarte per S-ID-Check-App. Bitte beachten Sie, dass die Aufforderung zur Zahlungsbestätigung per App nicht bei jedem Online-Einkauf abgefragt wird.

Wichtig: Wir empfehlen, Ihre Kreditkarte in jedem Fall für den S-ID-Check zu registrieren. Der Online-Einkauf generell wird aufgrund von rechtlichen Anforderungen in Kürze nur noch mit Karten gestattet sein, die für den S-ID-Check registriert sind.

* Aus Gründen der besseren Lesbarkeit wird hier in der gesamten Broschüre von der Kreditkarte gesprochen. Sämtliche Angaben gelten gleichermaßen auch für die Mastercard/Visa Basis (Debitkarte).

Sicherheitstipps

- Prüfen Sie die Allgemeinen Geschäftsbedingungen des Online-Anbieters.
- Geben Sie Ihre Kreditkartennummer nur im konkreten Bezahlvorgang an, niemals zur einfachen Identifikation Ihrer Kundendaten bzw. um Zutritt zu einem Internetaccount zu erlangen.
- Bestellen Sie nur bei Anbietern, die ihre Kommunikation mit SSL absichern. Dies erkennen Sie an dem Schlosssymbol in der Kopfzeile des Browsers.
- Verwenden Sie für Online-Einkäufe mit Kreditkarte immer Mastercard® Identity Check™ bzw. Visa Secure.
- Speichern Sie die Bestätigung zu jedem Bestellvorgang sicher ab. Bei Kündigung eines Internetservice bewahren Sie eine Kopie der E-Mail auf.
- Schreiben Sie Ihr Kennwort nicht auf bzw. speichern Sie es nicht ab.
- Achten Sie darauf, dass niemand die Eingabe Ihres Kennworts sieht, beispielsweise in der Öffentlichkeit.
- Seien Sie misstrauisch, an wen Sie Ihre Zugangsdaten weitergeben. Ihre Sparkasse wird Sie niemals auffordern, Ihre Zugangsdaten wie z. B. PIN, TAN oder Passwörter für Gewinnspiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen einzugeben. Antworten Sie daher nie auf solche Anfragen.
- Wenden Sie sich bei Bedarf an Ihre Sparkasse, um den Verfügungsrahmen für Ihre Online-Einkäufe zu begrenzen.
- Kommt Ihnen im Bestellprozess etwas ungewöhnlich vor oder vermuten Sie den Missbrauch Ihrer Daten, kontaktieren Sie uns bitte umgehend. Wählen Sie den Sperr-Notruf 116 116, um Ihre Kreditkarte oder Ihren Online-Banking-Zugang zu sperren. Genauere Informationen hierzu erhalten Sie auf der Rückseite dieser Broschüre.

Wie erkennen Sie Gefahren aus dem Internet?

Es gibt einige Gefahren aus dem Internet, vor denen Sie auf der Hut sein sollten. Die häufigsten Betrugsfälle sind:

Pharming
So merken Sie es: Die Startseite weist nicht die typischen Sicherheitsmerkmale auf – in der Adresszeile fehlt das Kürzel „https“. Eventuell haben Schrift und Symbole andere Farben oder eine andere Größe als sonst. Das steckt dahinter: Möglicherweise sind Sie Opfer einer Pharmingattacke geworden. Dabei manipuliert eine Schadsoftware Ihren Computer. Sie leitet Verbindungsversuche, beispielsweise zur Sparkassen-Website, auf eine gefälschte Internetseite um, die der Originalseite täuschend ähnlich sieht. Ziel ist es, Ihre Kontodaten, PIN oder Kartendaten zu stehlen. Pharming gelingt aber nur, wenn zuvor die Schadsoftware auf Ihrem Computer installiert wurde – z. B. in Form eines Trojaners.

Trojaner
Trojaner sind Spionageprogramme, die das Verhalten Ihres PCs beim Online-Banking verändern. Sie gelangen beispielsweise über Downloads im Internet oder beim Öffnen unsicherer E-Mail-Anhänge auf den Computer. Trojaner fragen beispielsweise über eine gefälschte Internetseite TANs oder Kartendaten von Ihnen ab. Aber Vorsicht: Diese Daten fließen an Datendiebe, um beispielsweise unbemerkt eine Überweisung von Ihrem Konto durchzuführen oder mit Ihren Kartendaten bei Online-Händlern einzukaufen. Eine besonders gefährliche Variante des Trojaners manipuliert unbemerkt die von Ihnen eingegebenen Überweisungsdaten. Achten Sie daher auf Unstimmigkeiten bei der TAN-Eingabe – erkennbar beispielsweise durch einen abweichenden Zahlungsbetrag. Brechen Sie den Zahlungsvorgang in diesem Fall lieber ab und kontaktieren Sie uns sofort.

Gute Virenscanner erkennen die meisten Trojaner. Deshalb sollten Sie Ihren PC regelmäßig mit einem aktuellen Virenscanner überprüfen.

Das Aussehen von falschen E-Mails wirkt oft professionell und integriert die Logos von Geldinstituten oder Online-Shops. Warnhinweise können hier sein:

– Kryptische und untypische Absenderadresse.

– Rechtschreibfehler im Text bzw. falsche Umlaute oder kyrillische Buchstaben.

– Falsche Grammatik.

– Keine persönliche Anrede (beispielsweise nur „Sehr geehrter Herr!“).

Social Engineering

Beim sogenannten „Social Engineering“ nutzen Betrüger den „Faktor Mensch“, also menschliche Eigenschaften wie Hilfsbereitschaft, Pflichtbewusstsein, Vertrauen oder auch Angst, aus, um sich vertrauliche Informationen und Daten illegal zu erschleichen. Sie täuschen dabei falsche Identitäten vor und geben sich beispielsweise als Mitarbeitende eines Telefonanbieters, Finanzamts oder der Sparkasse aus. Die Opfer werden dazu manipuliert, ihre Zugangsdaten preiszugeben oder Überweisungen auszuführen. Die Betrüger spielen ihre Rolle dabei meist so authentisch, dass Opfer die vermeintliche Manipulation nicht als solche erkennen. Seien Sie deshalb vorsichtig, wenn Sie von Fremden per E-Mail oder Telefon kontaktiert werden, und geben Sie niemals vertrauliche Informationen wie Passwörter weiter. Kein seriöses Unternehmen oder Finanzinstitut wird Sie hierzu auffordern.

Phishing

Eine besonders häufige Form des Social Engineerings ist das „Phishing“. Bei diesem „Passwort-Fischen“ erhalten Sie beispielsweise E-Mails von vermeintlichen Beratern oder Beraterinnen Ihrer Sparkasse, in denen Sie über einen Internetlink auf eine gefälschte Internetseite der Sparkasse gelockt werden. Dort werden Sie dazu aufgefordert, Ihre Zugangsdaten und eine TAN in ein Formular einzugeben. Diese Daten nutzen die Betrüger, um illegale Abbuchungen von Ihrem Konto vorzunehmen. Auch über Fax oder Telefon versuchen Betrüger, Ihnen Ihre geheimen Zugangsdaten fürs Online-Banking oder Kartendaten zu entlocken. In jedem Fall gilt: Geben Sie niemals Ihre geheimen Daten preis.

Weiterführende Informationen zur Sicherheit im Internet erhalten Sie unter: www.bsi-fuer-buerger.de.

Fit für das Internet

- → Aktualisieren Sie regelmäßig das Betriebssystem und die eingesetzten Programme auf Ihren Geräten wie Laptop und Smartphone.
- → Arbeiten Sie nicht mit Administratorrechten auf Ihrem Computer.
- → Halten Sie Firewall und Virenscanner immer aktuell.
- → Löschen Sie nach Online-Finanzgeschäften immer Ihren Browserverlauf und Cache. Noch besser: Nutzen Sie den „privaten Modus“ oder „Inkognito-Modus“. Denn so wird erst gar keine Historie Ihrer Online-Finanzgeschäfte angelegt.
- → Schützen Sie Ihre mobilen Endgeräte vor unberechtigten Zugriffen mit einer Code-Sperre.
- → Erledigen Sie Bankgeschäfte oder Online-Einkäufe nie über ein fremdes WLAN.
- → Hinterlegen Sie keine persönlichen Zugangsdaten auf Ihrem Rechner und auf fremden Portalen. Schreiben Sie Ihre Daten nicht auf und geben Sie diese nicht an Dritte weiter.
- → Achten Sie darauf, dass Sie Online-Finanzgeschäfte nur über eine verschlüsselte Verbindung tätigen. Diese erkennen Sie an dem Schlosssymbol im Browserfenster.
- → Tippen Sie die Internetadresse beim Online-Banking oder bei Online-Einkäufen immer manuell ein.
- → Öffnen Sie keine Links oder Dateianhänge in E-Mails von unbekannten Absendern.
- → Folgen Sie nie Aufforderungen, die Sie per E-Mail oder Telefon erhalten, Zahlungsaufträge zu bestätigen.

Sichere Kommunikationswege

Nutzen Sie keine unverschlüsselten E-Mails. Diese Nachrichten können im Internet von Dritten mitgelesen werden. Für eine sichere Kommunikation mit uns stehen Ihnen auf unserer Internetseite Kontaktformulare zur Verfügung, über die Ihre Nachricht verschlüsselt an uns übertragen wird.

Wichtige Informationen zu Veränderungen bezüglich Ihres Online-Bankings und der verwendeten Sicherungsverfahren erhalten Sie von uns ausschließlich postalisch, als Nachricht über Ihr Elektronisches Postfach im Online-Banking oder als verbindliche Information auf unserer Internetseite. In solchen Fällen werden wir Sie niemals über eine E-Mail informieren. Bitte reagieren Sie daher nie auf vermeintliche Aufträge und Anfragen per E-Mail, die vorgeben, von der Sparkasse zu stammen. Bitte öffnen Sie niemals die Anhänge von solchen E-Mails.

Was tun im Notfall?

Bei Verlust, Diebstahl oder Verdacht auf Missbrauch lassen Sie Ihre Karte oder Ihren Online-Banking-Zugang bitte sofort sperren über den zentralen Sperr-Notruf:

116 116

Diese Nummer ist rund um die Uhr und innerhalb von Deutschland kostenfrei für Sie erreichbar.

Im Ausland wählen Sie in der Regel +49 116 116. Bitte informieren Sie sich vor Reiseantritt über eine möglicherweise abweichende Ländervorwahl (www.sperr-notruf.de).
Die Höhe der Gebühren ist abhängig vom ausländischen Anbieter/Netzbetreiber.

Bei Verlust Ihrer Karte
Sie haften bis maximal 50 Euro je Karte, sofern Sie Ihre Mitwirkungs- und Sorgfaltspflichten eingehalten und die Sperrung Ihrer Karte unverzüglich veranlasst haben.

Ihr Weg zu uns
Wir sind für Sie da. Kommen Sie in Ihre nächstgelegene Sparkassen-Filiale oder informieren Sie sich online unter www.sparkasse.de.