

Suresse
Direkt Bank



Sicheres Online-Banking



Gemeinsam sind wir stärker

Inhaltsverzeichnis

Online-Sicherheit, eine gemeinsame Verantwortung	03
Santander Consumer Bank: eine sichere Online-Umgebung	04
Online-Sicherheit gehört zu unserer DANN	04
Unsere Online-Sicherheitsverfahren	05
Wie können Sie sich im Internet schützen?	07
Beim Passwort lohnt sich Sorgfalt	07
Achtung vor Phishing	07
... Smishing: Betrug per SMS	09
Erst nachdenken, dann teilen	10
Ein schöner Moment ist schnell geteilt	11
Lassen Sie die Technik für sich arbeiten	12
Etwas Verdächtiges entdeckt? Sofort melden!	13



Online-Sicherheit, eine gemeinsame Verantwortung



In den vergangenen Jahren haben Unternehmen, Organisationen und Behörden ihre Dienstleistungen zunehmend digitalisiert. Auch im Bankensektor ist die Digitalisierung deutlich erkennbar. Ob Direktbank oder klassische Filialbank, es setzen beide verstärkt auf Apps und digitale Anwendungen mit nur den höchsten Sicherheitsstandards. Damit Sie Ihre Bankgeschäfte online sicher durchführen können, gilt für uns eine konsequente Ausrichtung auf IT-Sicherheit und deren kontinuierliche Weiterentwicklung.

Und trotzdem bleibt Online-Sicherheit immer eine gemeinsame Verantwortung: Ihre Bank sorgt für die geschützte Umgebung – den entscheidenden Unterschied machen aber Sie selbst, mit dem richtigen Online-Wissen und bewussten Gewohnheiten. In diesem E-Book zeigen wir Ihnen, wie wir gemeinsam für sicheres Online-Banking sorgen. Sie erfahren, welche Sicherheitsmaßnahmen von der Santander Consumer Bank umgesetzt werden und worauf Sie selbst achten sollten, um Betrugsversuchen vorzubeugen.

Suresse Direkt Bank: eine sichere Online-Umgebung

Das Internet eröffnet unzählige Möglichkeiten und Chancen – als Online-Bank machen wir uns diese mit Überzeugung zunutze. Doch mit diesen Möglichkeiten geht auch eine gesellschaftliche Verantwortung einher. Bei der Santander Consumer Bank arbeiten wir daher kontinuierlich an einem sicheren Umfeld für das Online-Banking für Privatkunden sowie Geschäftskunden.

Online-Sicherheit gehört zu unserer DNA

Gemeinsam lassen wir Cyberkriminellen keine Chance. Das gilt nicht nur für unsere Kundinnen und Kunden, sondern auch für unsere internen Prozesse. Online-Betrug kennt keine Grenzen – unser Schutz auch nicht: Als eine internationale Gruppe sorgen wir gemeinsam für höchste Cybersicherheit.

Bei der Suresse Direkt Bank wollen wir aufklären und sensibilisieren – damit Online-Sicherheit für alle selbstverständlich wird. Für ein Internet, in dem Bankgeschäfte für alle sicher sind. Und dieses Bewusstsein beginnt natürlich bei unseren Mitarbeitenden. Workshops, Phishing-Tests, Live-Hacking: Als Gruppe schulen wir unsere Mitarbeitenden kontinuierlich weiter. Damit Bedrohungen schnell auffallen – und ebenso schnell an die zuständige Meldestelle gehen.

Haben Sie Fragen zum Online-Banking? Nachricht angeblich von uns – aber Sie sind unsicher und zweifeln daran? Unser Kundenservice unterstützt Sie gerne und beantwortet Ihre Fragen werktags von 9 bis 18 Uhr – telefonisch, per E-Mail oder per Formular.



Unsere Online-Sicherheitsverfahren

IT-Sicherheit? Da kennen wir bei der Suresse Direkt Bank keine halben Sachen. Wir haben eine Reihe gezielter Sicherheitsverfahren entwickelt – damit Cyberkriminelle gar nicht erst zum Zug kommen.

Gesicherte Überprüfung von Identität und Kontaktdaten

Bei der Eröffnung eines Online-Sparkontos stellen wir eine Verknüpfung zwischen der Identität des Kunden und seinen Kontaktdaten her. Dazu verwenden wir WebID oder Postident. Auch bei der Änderung von Daten kommen diese Sicherheitsverfahren zum Einsatz.

“
**Bei der Suresse
Direkt Bank machen wir
in Sachen IT-Sicherheit
keine halben Sachen.**
”



Persönlicher Zugangscode für Ihr Sparkonto

Nach der Eröffnung Ihres Sparkontos erhalten Sie von uns eine E-Mail mit Ihrer Kontonummer, Ihrem Benutzernamen und einem vorläufigen Zugangscode. Damit dieser Zugangscode nicht missbraucht werden kann – beispielsweise bei einem kompromittierten E-Mail-Konto – verwenden wir ausschließlich zeitlich begrenzte Zugangsdaten.

Der Code aus unserer E-Mail gilt nur für den ersten Zugang: Sobald Sie sich anmelden, wählen Sie Ihren persönlichen Code. Zu Ihrer Sicherheit funktioniert das ausschließlich mit einem Passwortschlüssel, den Sie per SMS auf Ihrer hinterlegten Telefonnummer erhalten. Ihre Telefonnummer lässt sich nur über ein streng gesichertes Verfahren ändern. So bleibt Ihr Zugang jederzeit geschützt.

Überweisungen ausschließlich auf Ihr Referenzkonto

Bei der Eröffnung eines neuen Online-Sparkontos wird dies mit Ihrem Referenzkonto verbunden. Dabei handelt es sich um ein Girokonto, das bei einer anderen Bank auf Ihren Namen läuft. Auszahlungen von Ihrem Sparkonto bei der Suresse Direkt Bank erfolgen ausschließlich per Überweisung auf Ihr Referenzkonto.

Sollten Sie dieses Referenzkonto online ändern wollen, muss zunächst eine Überweisung vom neuen Referenzkonto auf Ihr Sparkonto bei Suresse Direkt Bank erfolgen. Dadurch können wir Ihre Identität erneut eindeutig feststellen.

Einmaliger SMS-Code für jede Transaktion

Für die Anmeldung zu Ihrem Online-Banking benötigen Sie lediglich Ihren Benutzernamen und Ihren persönlichen Zugangscode. Bei Überweisungen auf Ihr Referenzkonto oder der Änderung Ihrer persönlichen Daten benötigen Sie zusätzlich einen einmaligen SMS-Code. Dieser Sicherheitscode wird an die Mobiltelefonnummer gesendet, die Sie bei der Kontoeröffnung angegeben haben.



Wir haben eine Reihe gezielter Sicherheitsverfahren entwickelt – damit Cyberkriminelle gar nicht erst zum Zug kommen.



Wie schützen Sie sich im Internet?

Für die Sicherheit beim Online-Banking sorgen die Sicherheitslösungen der Banken. Mindestens ebenso wichtig ist jedoch, wie Sie selbst damit umgehen. Die Methoden von Cyberkriminellen werden immer ausgefeilter – mit einem wachsamem Blick haben Sie das Risiko dennoch gut im Griff. Hier finden Sie die wichtigsten Tipps auf einen Blick.

Beim Passwort lohnt sich Sorgfalt

Dass Nachname und Geburtsdatum tabu sind und jedes Konto sein eigenes Passwort braucht, wissen Sie längst. Der wichtigste Tipp ist aber ein anderer: Setzen Sie lieber auf Länge als auf Komplexität – ein langes Passwort schlägt jede verschachtelte Zeichenfolge. Überraschend, aber wahr: An „huhnhundkatzekananinchenvogel“ beißen sich Angreifer jahrhundertlang die Zähne aus – „Ng3h7!a/“ kann dagegen schon nach drei Tagen entschlüsselt sein.

Achtung vor Phishing ...

Mit gefälschten E-Mails versuchen Betrüger, an persönliche Daten oder Ihr Geld zu kommen. Besonders gern schlüpfen sie in die Rolle vertrauenswürdiger Absender: Banken, Behörden oder Internetanbieter. Doch wie lassen sich gefälschte E-Mails von echten unterscheiden?

- Überprüfen Sie die E-Mail-Adresse des Absenders gründlich. Ein verräterisches Detail: Statt einer offiziellen Bankadresse steht dort oft eine allgemeine Adresse wie @gmail.com oder @mail.com. Ein zweiter Blick lohnt sich: Aus Santander wird schnell einmal satnander – und genau darauf setzen die Absender.



Wählen Sie ein neues Passwort

zwischenersuppeunddenkartoffeln 

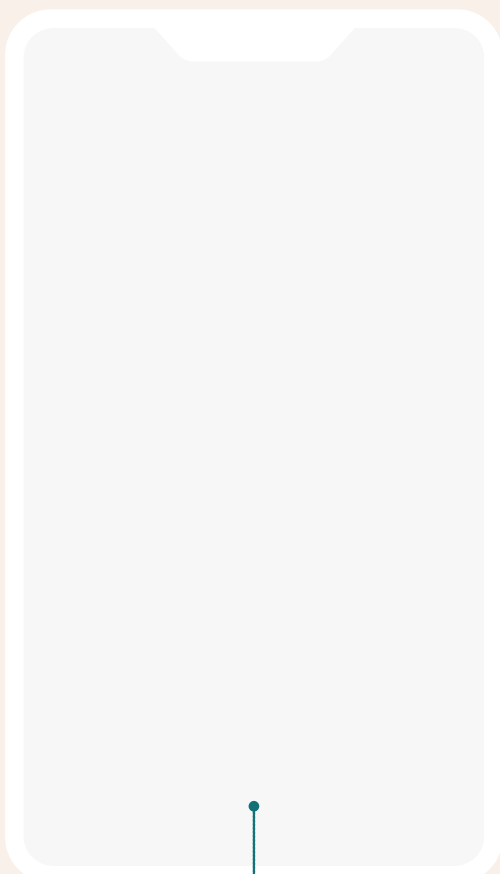
Wählen Sie ein neues Passwort

53j7!H 

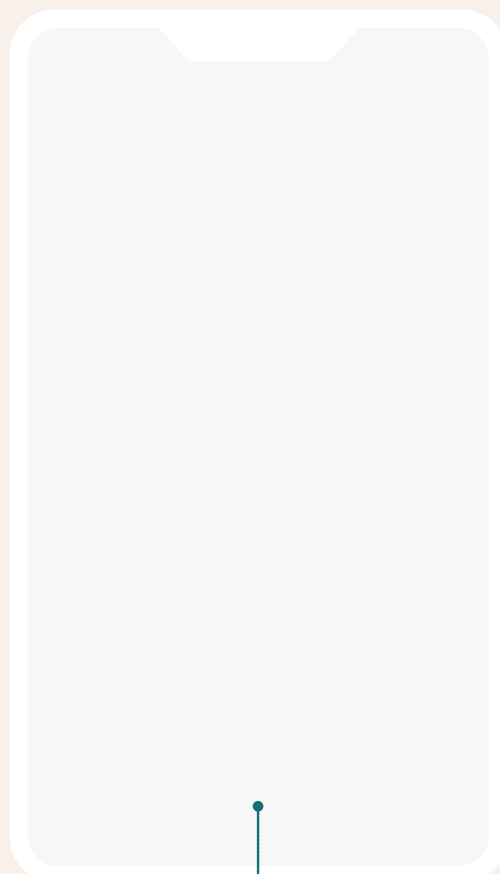
Zeit für ein neues Passwort?
Dann ist obiger Vorschlag die bessere Option.

EIN PAAR TIPPS

- Wer Sie zur Eile treibt, hat selten Gutes im Sinn: Phishing-Mails setzen auf Ultimaten und Drohungen. Mal wird mit der Sperrung Ihres Kontos gedroht, mal mit einer Geldstrafe – beides ist frei erfunden.
- Seriöse Organisationen fragen niemals per E-Mail nach vertraulichen Daten. Wenn Sie also eine unerwartete E-Mail erhalten, in der nach Bankdaten, Passwörtern, Adressen oder Ihrer Nationalregisternummer gefragt wird, sollten Sie besser auf der Hut sein.
- Prüfen Sie nicht nur die Adresse, sondern auch den Text selbst auf Rechtschreib- und Grammatikfehler. Cyberkriminelle versenden ihre betrügerischen E-Mails rund um den Globus – oft ohne ein Wort der Landessprache zu sprechen.
- Phishing-E-Mails enthalten manchmal auch einen Anhang. Dahinter steckt mit großer Wahrscheinlichkeit Schadsoftware, die Daten und sogar Geld von den Rechnern und Mobilgeräten der Betroffenen abgreift. Hier gilt: Finger weg, nicht öffnen und ab in den Papierkorb.



Diese E-Mail bezieht sich auf eine unbezahlte Rechnung, ohne Nennung weiterer Informationen. Sie erhalten auch ein Ultimatum: Zahlen Sie jetzt oder Ihr Konto wird geschlossen. Seriöse Absender setzen Sie nicht unter Zeitdruck. Bleiben Sie deshalb gelassen – und wachsam.



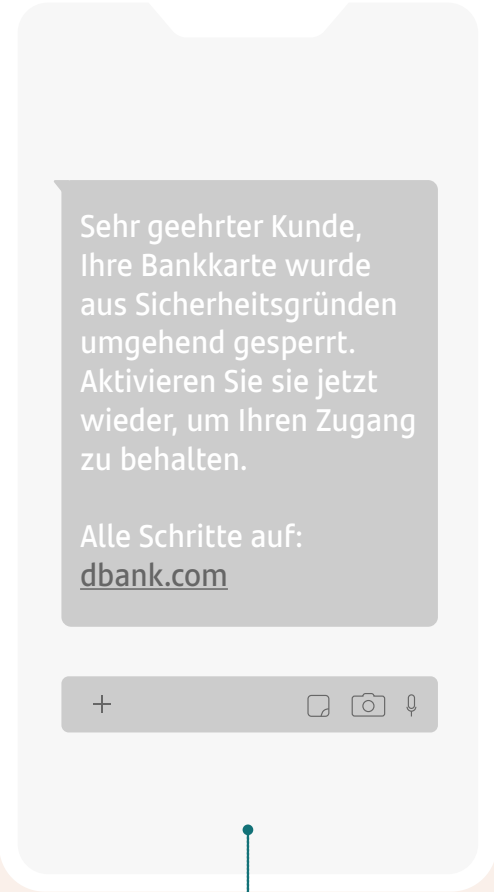
Der Paketdienst dpost als Absender? Die Endung @mail.com verrät die Fälschung. Auch Schreibfehler sollten Sie hellhörig machen.

... Smishing: Betrug per SMS

Phishing ist nicht nur auf E-Mails beschränkt. SMS und Messenger-Nachrichten wie bei WhatsApp werden ebenfalls für den Diebstahl von Daten und Geld eingesetzt. Auch hier tarnen sich die Täter als Bank, Unternehmen oder Behörden.

Eine weitere Betrugsmasche ist, sich als Familienmitglied auszugeben. Geben Sie auch per Nachricht nie vertrauliche Daten weiter. Vorsicht bei Angehörigen, die sich mit neuer Nummer melden und sofort das Löschen der alten Nummer oder eine Überweisung verlangen.

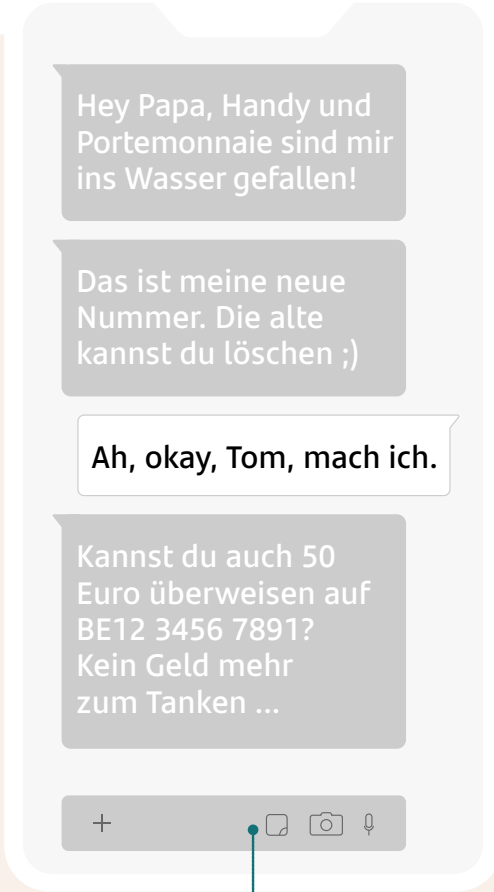
Zusätzlicher Tipp: Der Vorname fehlt: Cyberkriminelle geben sich zwar als jemand aus, den Sie kennen, den Namen nennen sie aber nie. Seien Sie wachsam bei solchen Nachrichten.



Sehr geehrter Kunde,
Ihre Bankkarte wurde
aus Sicherheitsgründen
umgehend gesperrt.
Aktivieren Sie sie jetzt
wieder, um Ihren Zugang
zu behalten.

Alle Schritte auf:
dbank.com

Banken werden Sie niemals per SMS auffordern, online vertrauliche Daten preiszugeben. Haben Sie eine solche Nachricht erhalten? Bitte wenden Sie sich an Ihre Bank, bevor Sie auf jedweden Link klicken.



Hey Papa, Handy und
Portemonnaie sind mir
ins Wasser gefallen!

Das ist meine neue
Nummer. Die alte
kannst du löschen ;)

Ah, okay, Tom, mach ich.

Kannst du auch 50
Euro überweisen auf
BE12 3456 7891?
Kein Geld mehr
zum Tanken ...

Der elterliche Reflex zu helfen ist genau das, worauf die Masche zielt. Dabei liegen die Warnzeichen offen: kein Name, die Bitte um Löschen der alten Nummer, die sofortige Geldforderung auf ein fremdes Konto zu überweisen.

Erst nachdenken, dann teilen

Unsichere Internetverbindungen sind der Spielplatz von Cyberkriminellen. In einem ungesicherten Netzwerk fällt es Kriminellen wesentlich leichter, sich Zugang zu Ihren Geräten zu verschaffen – ob Computer, Tablet oder Smartphone. In der Gastronomie können Sie oft kostenlos im Gäste-WLAN surfen. Bequem ist das zweifellos. Nur sind diese Netzwerke oft ungesichert. Meiden Sie offene Netzwerke und gehen Sie stattdessen über Ihre mobilen Daten ins Netz.

WLAN



Netzwerk



Kostenloses WLAN im Café



Hotel Iwis



Mein persönlicher Hotspot

Café statt Büro? Gern – aber nicht über das kostenlose, ungesicherte WLAN arbeiten. Verwenden Sie mit Ihrem Smartphone einen persönlichen Hotspot und nutzen Sie Ihre mobilen Daten zum Surfen.

WLAN



Netzwerk



Kostenloses WLAN im Café



Hotel Iwis



Mein persönlicher Hotspot

http://dewebshop.de/herrenkleidu

dewebshop

Suchen

Herrenbekleidung



Kurze Hose

Kurze Hose mit hohem Bund. Auch in Blau erhältlich.

€25

Jetzt bestellen!



T-shirt

Fällt großzügig aus. In verschiedenen Farben erhältlich!

€30

Jetzt bestellen!

Auf den ersten Blick ist an diesem Webshop nichts Auffälliges. Doch werfen Sie einen Blick auf die Adresszeile / URL, bevor Sie Ihre Daten eingeben: Sie zeigt, dass die Verbindung nicht gesichert ist.

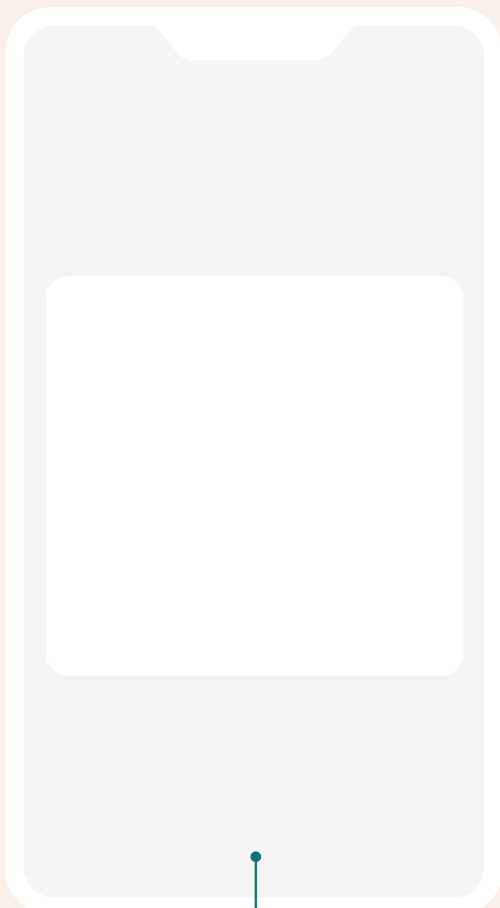
Ein prüfender Blick auf die Adresszeile gehört dazu – ob Sie eine Website besuchen oder etwas im Netz bestellen. Sichere Webseiten erkennen Sie am Schloss-Symbol in der Adresszeile Ihres Browsers.

Ein einziger Buchstabe macht den Unterschied: Nur bei „https://“ ist die Verbindung verschlüsselt, Adressen mit „http://“ nicht.

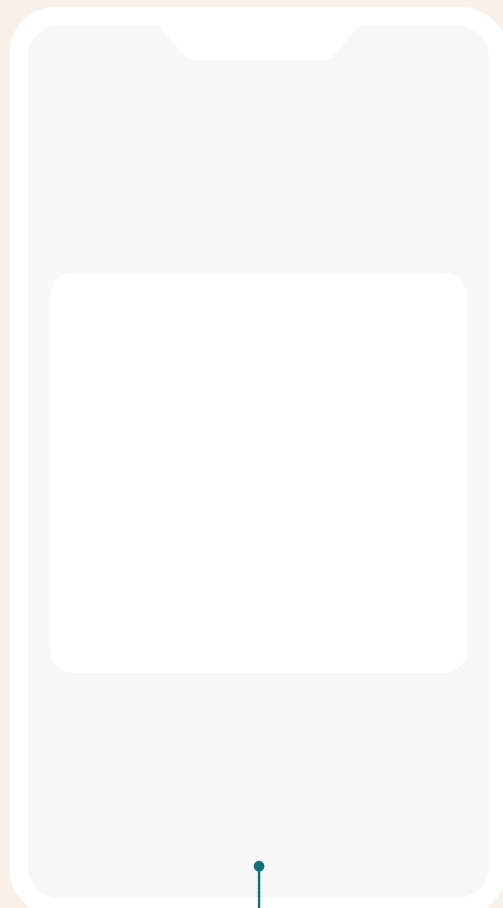
Ein schöner Moment ist schnell geteilt

Auf Facebook, Instagram und TikTok lassen sich schöne Augenblicke im Handumdrehen mit Familie, Freunden und Bekannten teilen. Genau deshalb lohnt der kurze Gedanke davor: Was zeigt dieses Foto/das Video eigentlich alles? Ein harmloses Detail für Sie – ein wertvoller Hinweis für jemanden mit schlechten Absichten.

Ihr neues Zuhause im Netz zeigen? Gern, aber ohne Straßennamen und Hausnummer im Bild – und ohne gespeicherte Standortdaten aus dem Foto. Teilen Sie ein Foto von Ihrem Arbeitsplatz? Ein kurzer Blick lohnt sich: Was auf dem Bildschirm zu sehen ist, sieht am Ende auch Ihr Publikum mit.



Café statt Schreibtisch – wunderbar! Ein schönes Foto. Nur sollte Ihre Bankkarte besser nicht mit im Bild sein. Werfen Sie auch einen Blick auf Ihren Bildschirm – was dort steht, sollte niemand mitlesen können.



Ein Foto, ein Straßenschild, eine Hausnummer: Schon kennt jeder Ihre Adresse – auch die, die es nicht wissen sollten.

Lassen Sie die Technik für sich arbeiten

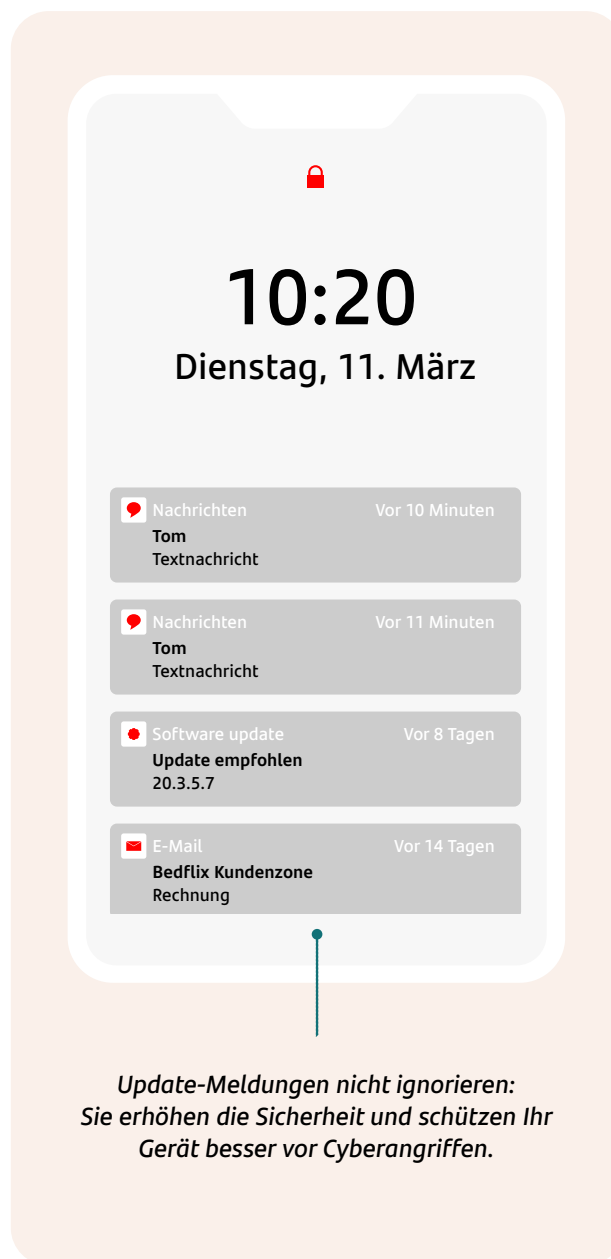
Zahlreiche Apps und Anwendungen schützen Laptop, Tablet und Smartphone vor Angriffen von außen. Spähsoftware, Schadprogramme und gefährliche Links werden dabei schon blockiert, bevor sie Schaden anrichten können. Der beste Schutz nützt nur, wenn er aktuell ist – halten Sie Software und Betriebssystem Ihres Geräts deshalb stets auf dem neuesten Stand. So bleibt Ihr Schutz immer auf dem neuesten Stand.



“

Halten Sie Software und Betriebssystem Ihres Geräts deshalb stets auf dem neuesten Stand.

”



Etwas Verdächtiges entdeckt? Verdachtsfälle sofort melden!

Eine seltsame E-Mail, ein verdächtiger Anruf oder eine merkwürdige Nachricht? Oder sind Sie bereits Opfer von Cyberkriminellen geworden? Dann sollten Sie den Vorfall bei den zuständigen Stellen melden. Es mag sich wie ein Tropfen auf den heißen Stein anfühlen – aber jede Meldung zählt. Gemeinsam sind wir stark.

Ihre Anlaufstellen?

Phishing oder Smishing melden

Vermuten Sie, dass Sie eine betrügerische E-Mail oder eine gefälschte Nachricht erhalten haben? Dann können Sie diese an www.online-strafanzeige.de weiterleiten. Anschließend sollten Sie die E-Mail oder die Nachricht am besten löschen.

Opfer von Cyberkriminalität?

Wurden Sie Ziel eines Cyberangriffs, sollten Sie das auf jeden Fall melden. Zögern Sie nicht aus Scham: Betrugsmaschen sind heute so ausgeklügelt, dass jeder darauf hereinkann.

Sie können sich auch direkt an die Polizei wenden: www.polizei.de





**Unsere Mitarbeiter stehen Ihnen an jedem Werktag
von 9:00 bis 18:00 Uhr telefonisch oder per E-Mail für Sie bereit.**



0800-100-1878



www.suessedirektbank.de



info@suessedirektbank.de

Suresse
Direkt Bank