

Willkommen in der Computeria Wallisellen



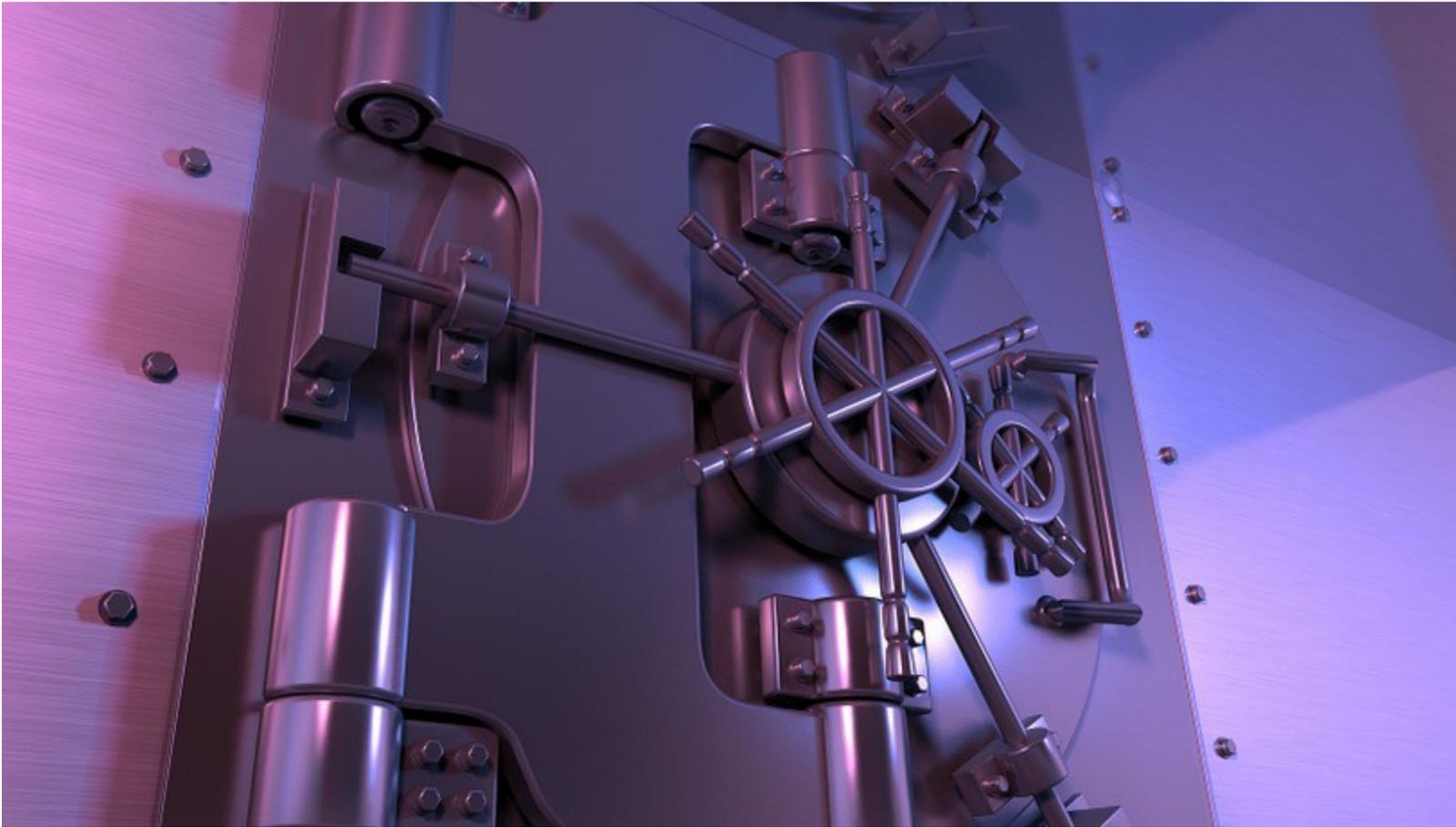
Sicher bezahlen

im Internet
eBanking
im Laden oder Restaurant
Kreditkarten oder Smartphone

Rolf Lehmann
15.1.2020



Wo ist Geld sicher ?



Einlagensicherung bei esisuisse

???

Wie sicher ist bezahlen?

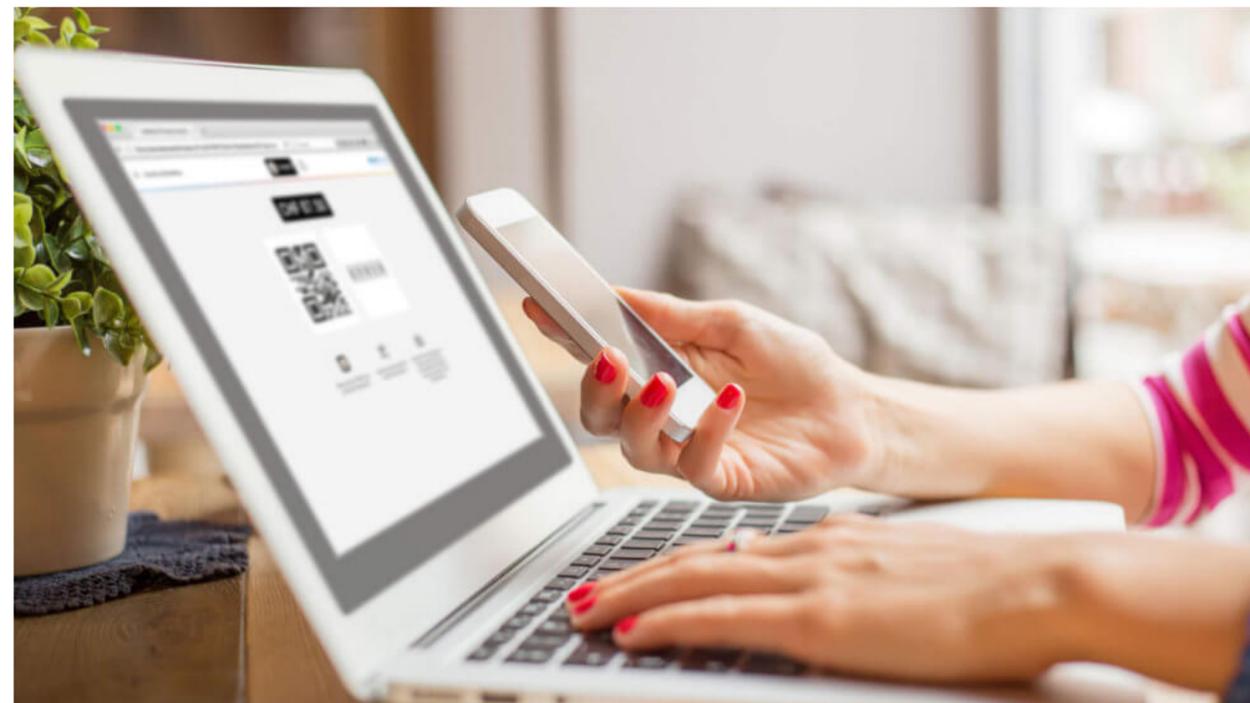
Bargeld



Kredit- und Debitkarten



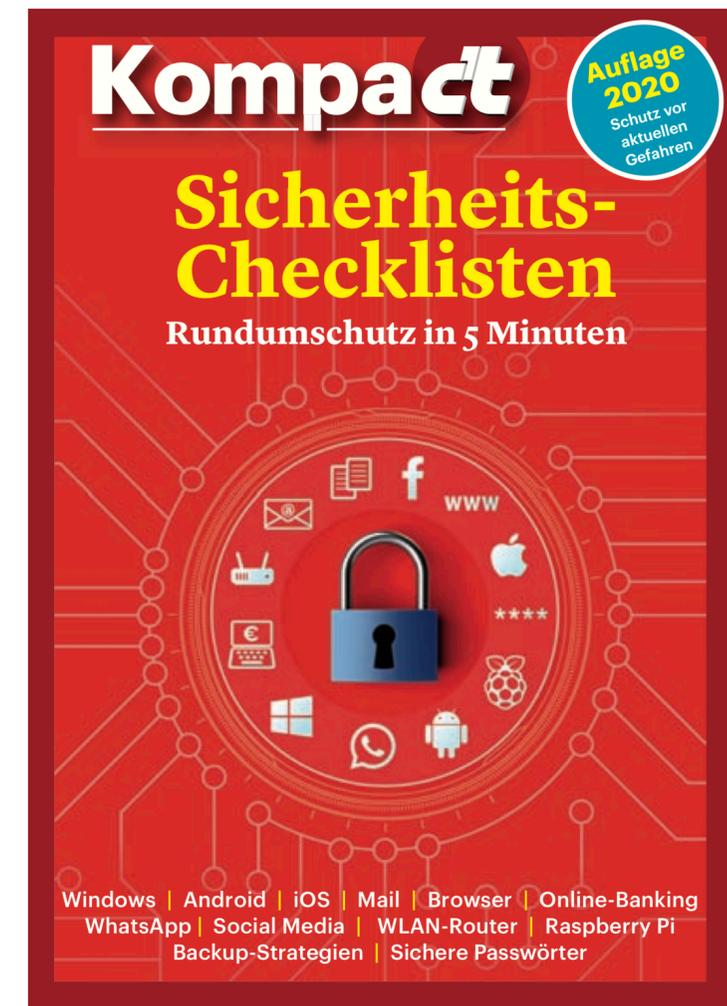
Smartphone, Tablet und Computer



Sicherheitsanforderungen

Checklisten für

- den PC
- das Smartphone oder Tablet
- das eBanking
- das Internet



Von den Profis: c't Sicherheits-Checklisten

Checkliste für den PC mit Windows 10

Was können Sie abhaken?

1 Windows updaten

Installieren Sie alle verfügbaren Updates, indem Sie „Updates“ ins Startmenü eintippen und auf „Nach Updates suchen“ klicken.

2 Virenschutz checken

Stellen Sie sicher, dass ein Virenschutz mit aktuellen Virensignaturen installiert ist. Der vorinstallierte Defender reicht aus. Seinen aktuellen Status erfahren Sie, indem Sie „Windows-Sicherheit“ über das Startmenü aufrufen und auf „Viren- & Bedrohungsschutz“ klicken.

Unbedingt Automatisches Update anwählen.

Checkliste für den PC mit Windows 10

Was können Sie abhaken?

3 Daten schützen

Erstellen Sie regelmässig Backups der wichtigsten Daten (siehe S. 16). Suchen Sie im Startmenü nach „Diagnose und Feedback“ und stellen Sie sicher, dass unter „Diagnosedaten“ die Option „Standard“ aktiv ist.

4 Software ausmisten

Deinstallieren Sie ungenutzte Anwendungen und bringen Sie alle anderen auf den aktuellen Stand. Das gilt insbesondere für Browser und Plug-ins, Mail-Clients, Office-Programme, PDF-Viewer und Multimedia-Player.

Checklisten Internet und eBanking

c't-Sicherheits-Checkliste

Web-Browser

Sicher surfen



✓ Aktuelle Version

Nutzen Sie stets die aktuelle Browser-Version, da in alten Versionen meist Sicherheitslücken klaffen. Stellen Sie sicher, dass der Browser automatisch mit Updates versorgt wird.

✓ Erweiterungen

Browser-Erweiterungen (auch Add-ons genannt) haben Zugriff auf alle angezeigten Webseiten (auch Online-Banking). Checken Sie vor der Installation die Nutzerbewertungen.

✓ Plug-ins meiden

Browser-Plug-ins wie Java und Silverlight sind längst überholt und potenziell unsicher. Deinstallieren Sie solche Plug-ins, wenn Sie noch welche auf Ihrem Rechner finden und nicht darauf angewiesen sind.

✓ https:// nutzen

Steuern Sie wann immer möglich die verschlüsselt übertragene https://-Version einer Website an. Hierbei hilft die Chrome- und Firefox-Erweiterung HTTPS Everywhere (siehe ct.de/check2020). Besuchen Sie eine Site nicht, wenn der Browser einen Zertifikatsfehler anzeigt.

✓ Berechtigungen

Websites fordern Berechtigungen an, um etwa Ihren Standort abzurufen. Erteilte Berechtigungen finden Sie bei den meisten Browsern, indem Sie in der Adressleiste links neben die Adresse klicken (meist Schloss-Symbol). Sortieren Sie alle Berechtigungen aus, die nicht länger nötig sind.

c't-Sicherheits-Checkliste

Online-Banking

Schutz für Ihre Bankgeschäfte



✓ Phishing erkennen

Online-Betrüger verschicken massenhaft Mails im Namen von Bankinstituten, um Trojaner einzuschleusen oder Zugangsdaten abzugreifen (Phishing). Geben Sie Ihre Zugangsdaten nur auf der Webseite der Bank oder in Ihrer Online-Banking-Software ein.

✓ Transaktion checken

Checken Sie bei Online-Überweisungen das Zielkonto und die Summe auf dem TAN-Generator, in der Banking-App oder auf dem Kartenleser und zusätzlich auf der Rechnung.

✓ Virenfreier Rechner

Online-Banking mit dem PC ist nur sicher, wenn das System virenfrei ist. Sorgen Sie dafür, dass ein Virens Scanner mit ak-

tuellen Updates aktiv ist. Unter Windows 8.1 und 10 reicht der vorinstallierte Defender aus.

✓ Belege überprüfen

Insbesondere Kreditkarten-Nutzer sollten regelmäßig die Abrechnung kontrollieren und unbefugte Abbuchungen umgehend an die kartenherausgebende Bank melden. Auch Ihre Kontoauszüge sollten Sie auf Auffälligkeiten untersuchen.

✓ Handy nicht rooten

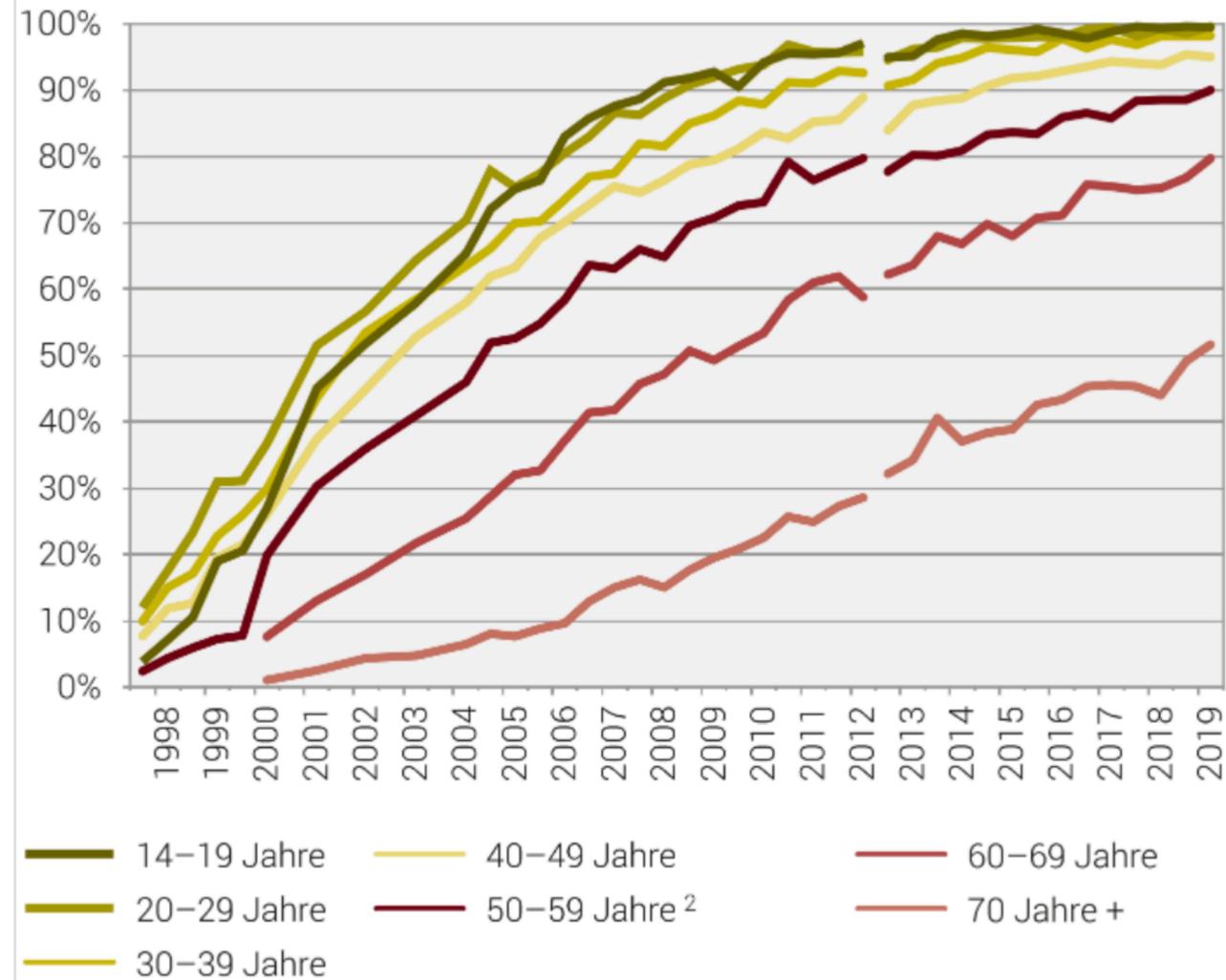
Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet nicht, da Sie damit wichtige Schutzfunktionen lahmlegen. Viele Banking-Apps starten auf modifizierten Geräten aus diesem Grund nicht.

Geräte aktuell halten
Regeln immer einhalten
Sicherheit hat oberste Priorität
Energie- und Zeitaufwand lohnt sich

Internetnutzung

Internetnutzung in der Schweiz nach Alter, Entwicklung¹

Regelmässige Nutzerinnen und Nutzer (ENK), in % der Personen ab 14 Jahren

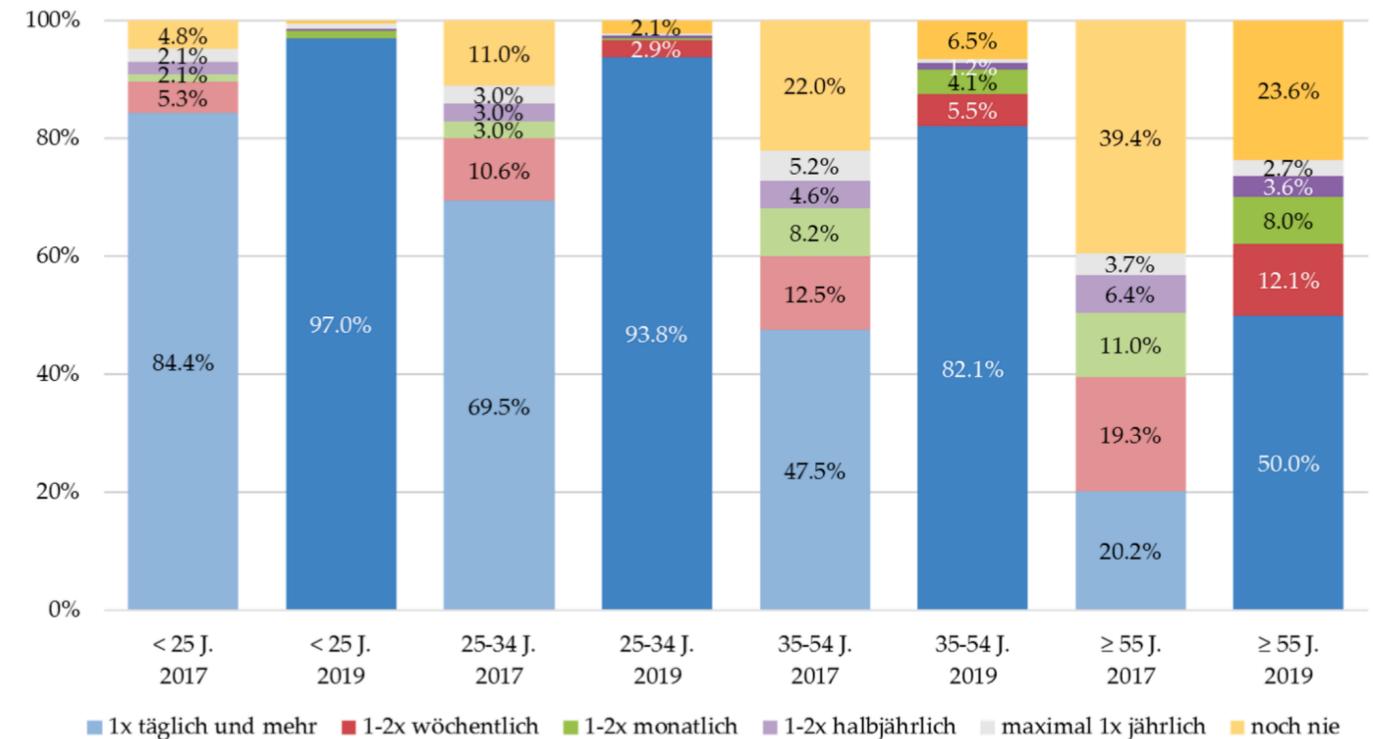


¹ Aus methodischen Gründen können die Ergebnisse ab Herbst 2012 nicht mit älteren Studien verglichen werden. Ein Vergleich mit den kommenden Jahren ist dagegen möglich
² ab 50 Jahren in den Jahren 1997-1999

Häufigkeit der mobilen Internetnutzung

Jahresvergleich nach Alter

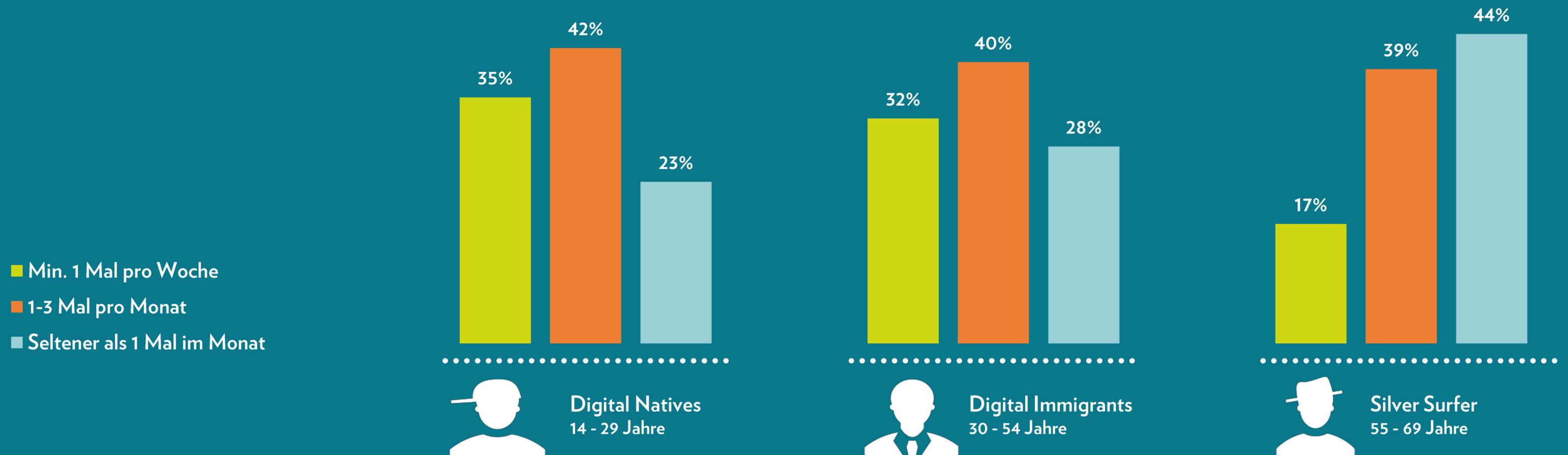
Wie oft greifen Sie über Ihr Mobiltelefon auf das Internet zu?



Quelle: Der Schweizer Online Handel Internetnutzung Schweiz 2019
 Forschungszentrum für Handelsmanagement, HSG

WIE OFT KAUFEN DIE SCHWEIZER ONLINE EIN?

Basis: Kernzielgruppe d.h. Personen, die online einkaufen.



TOP 5 GRÜNDE FÜR ONLINESHOPPING

Basis: Kernzielgruppe



Lieferung nach Hause

57%



24h Einkaufen

56%



Bessere Vergleichsmöglichkeiten

50%



Zeitersparnis

45%



Bequemer als im Laden

43%

ICH ZÖGERE BEIM ONLINE-KAUF WEIL...

Basis: Kernzielgruppe

65%

..mir die Versandkosten zu teuer sind

36%

..mir die Rückgabe der Produkte zu aufwendig ist

26%

..ich den Online-Shops nicht vertraue

49%

..ich dort Produkte nicht anfassen, anprobieren oder testen kann

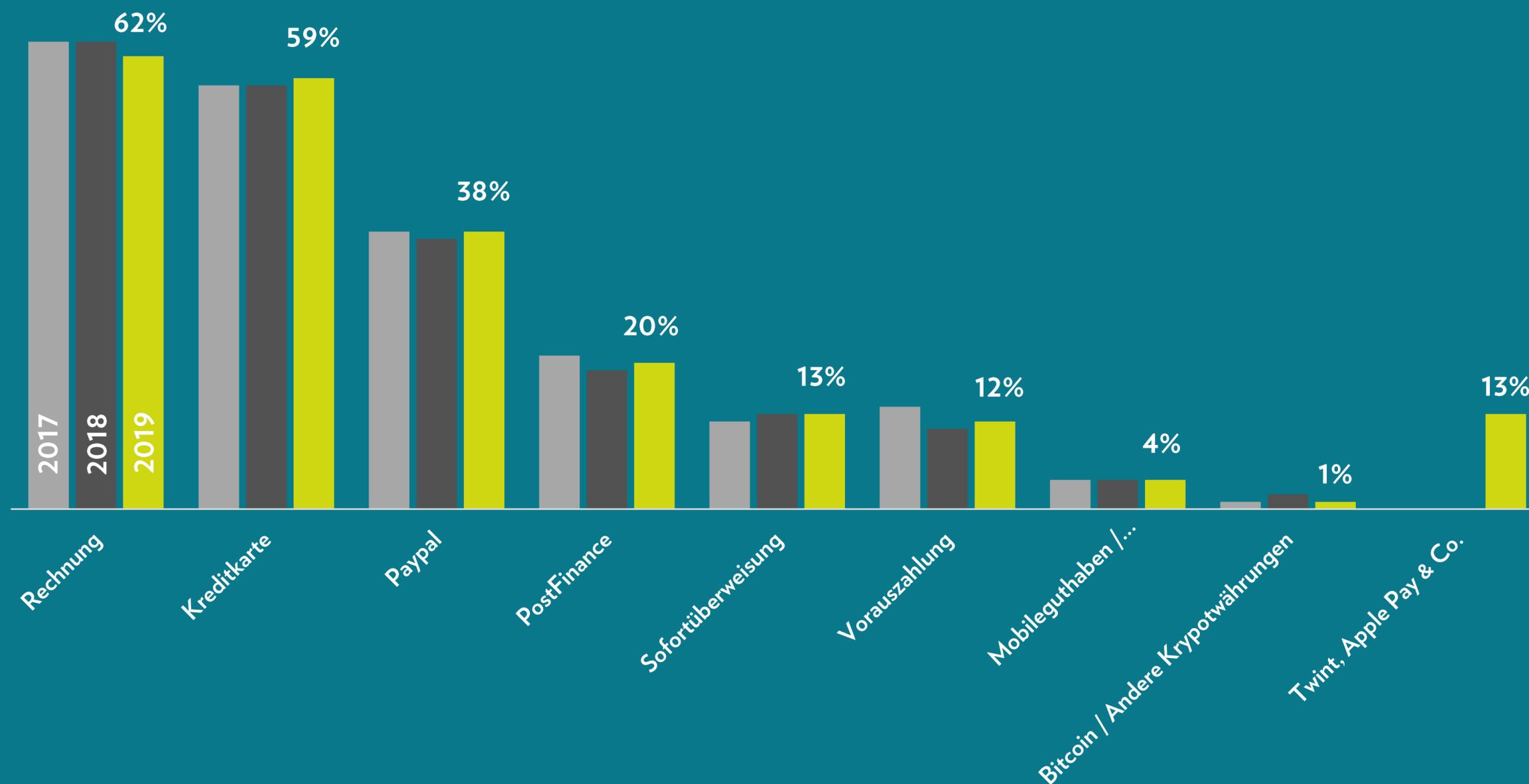
38%

..ich nicht finde, was ich suche

BEZAHLEN PER RECHNUNG BLEIBT SPITZENREITER

Bevorzugte Bezahlmöglichkeiten

Basis: Kernzielgruppe



Einkaufen im Internet

Die Schweizer kaufen am häufigsten bei Zalando, Amazon und Digitec ein. Fürs Onlineshopping geben sie im Durchschnitt 164 Franken aus, Total 12.2 Milliarden Franken im 2018

Über die Hälfte der Schweizer kaufen mindestens einmal pro Monat Waren und Dienstleistungen im Internet. Besonders häufig schlagen Millennials zwischen 25 und 34 Jahren online zu.

Rangliste Online Käufe

1. Zalando
2. Amazon
3. Digitec
4. Wish
5. ricardo.ch
6. AliExpress
7. Microspot
8. ex libris
9. Galaxus
10. SBB

Quelle: Der Schweizer Online Handel Internetnutzung Schweiz 2019
Forschungszentrum für Handelsmanagement, HSG

Beispiel 1: Einkaufen bei Coop@home

<https://www.coopathome.ch/>

1. Registrieren und dann Anmelden mit E-Mail-Adresse und Passwort

2. Einkaufen

3. Bezahlen

Zahlungsart wählen

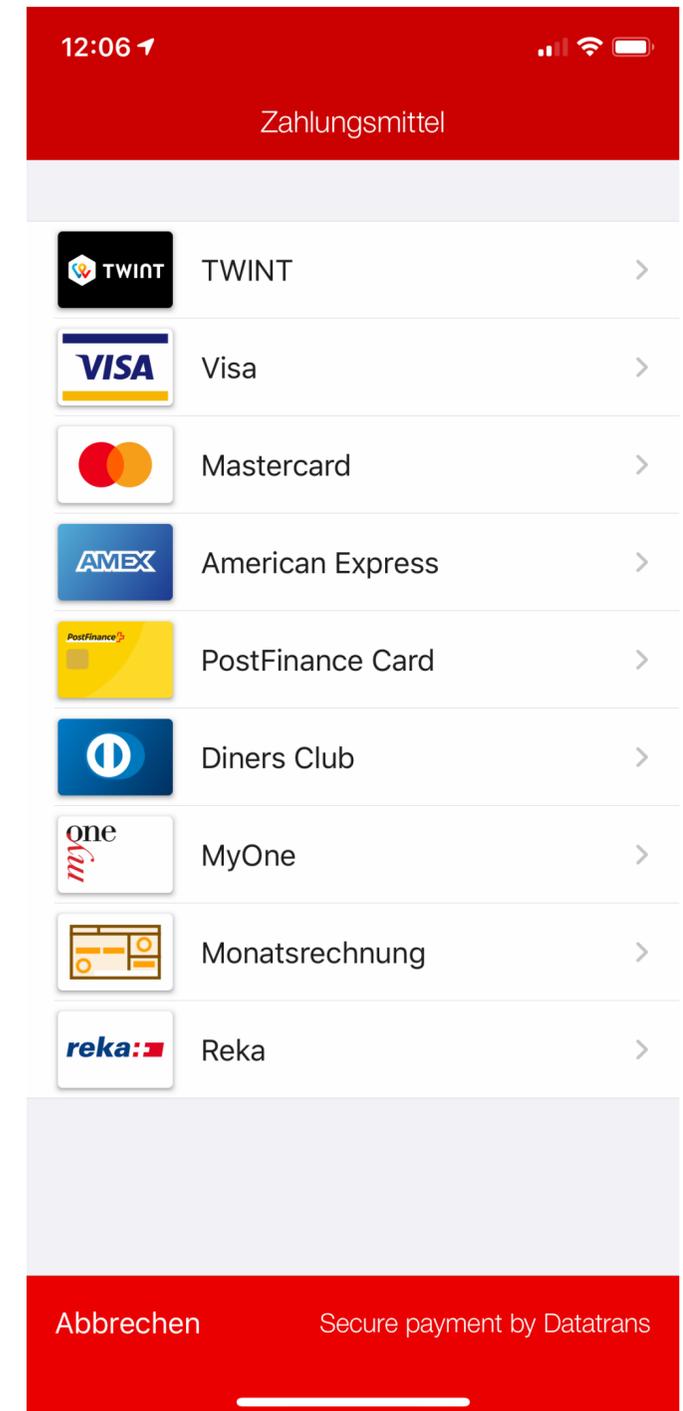
- Kreditkarte
- TWINT - Mobile Payment
- PostFinance
- Monatsrechnung PowerPay
- Rechnung per E-Mail

4. Abmelden

Beispiel 2: Einkaufen bei der SBB

<https://www.sbb.ch> oder SBB App

1. Registrieren und dann Anmelden mit E-Mail-Adresse und Passwort
Wer hat, SwissPass Infos hinterlegen
2. Zahlungsart in den Einstellungen wählen
3. Reise suchen und Billett auswählen
4. Bezahlen und reisen



Beispiel 3: Einkaufen bei Digitec

<https://www.digitec.ch>

1. Registrieren und dann Anmelden mit E-Mail-Adresse und Passwort als Sicherheitsoption kann Zwei-Faktor-Authentifizierung aktiviert werden (Google Authenticator App)
2. Einkaufen
3. Zahlungsart wählen
4. Bezahlen
5. Abmelden

2. Zahlung

Bitte wähle eine Zahlungsoption.

<input type="radio"/> TWINT	Kostenlos
<input type="radio"/> Kryptowährungen	Kostenlos
<input type="radio"/> PostFinance E-Finance	Kostenlos
<input type="radio"/> PayPal	2.00%
<input type="radio"/> PostFinance Card	Kostenlos
<input type="radio"/> Migros Bank	Kostenlos
<input type="radio"/> Rechnung	Kostenlos
<input type="radio"/> Vorauszahlung	Kostenlos
<input type="radio"/> Google Pay	Kostenlos
<input type="radio"/> Neue Kreditkarte	Kostenlos

eBanking

Alle Finanzinstitute bieten es an

Viele bieten Informationsanlässe und Kurse dazu an.

Führen Sie es zu Hause bzw. an einem sicheren Ort durch.

Das ist viel sicherer als Bargeld abheben und wieder einzahlen.

Nach ein paar mal üben funktioniert es schnell und sicher.

Komfortfunktionen

- Daueraufträge
- Zahlungsvorlagen
- elektronische Rechnung eBill

Mit dem Smartphone kommen weitere Komfortfunktionen dazu

- Authentifizierung mit Fingerabdruck bzw. Gesichtserkennung
- Einlesen der Einzahlungsscheine mit der Kamera
- Freigabe der Zahlungen mit dem Smartphone

Sorgfaltspflichten eBanking

1. Benutzen Sie nur die von der Bank angegebenen Kommunikationswege
2. Eine Bank wird Sie nie nach Benutzernamen, Konten und Passwörtern fragen.
3. Endgeräte sind auf dem aktuellen Stand, Betriebssystem, Browser, Virenschutz aktiv
4. Sichere Aufbewahrung der Kontoinformationen
5. Verlust, Diebstahl und Missbrauch sofort melden > Zugriff sperren
6. Geheimhaltung Passwörter
7. Prüfung der Kontoauszüge und Meldung von Missbrauch
8. Mitteilung von Änderungen
9. Immer korrekt abmelden und Verlauf löschen

2-Faktor bzw. Multifaktor Authentifikation

Definition:

Die **Zwei-Faktor-Authentisierung (2FA)**, häufig auch als *Zwei-Faktor-Authentifizierung* bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden, oder Passphrase und TAN beim Online-Banking. Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung.

PIN: Persönliche Identifikations Nummer, ein Mehrmalkennwort

TAN: Transaktionsnummer, ein Einmalkennwort

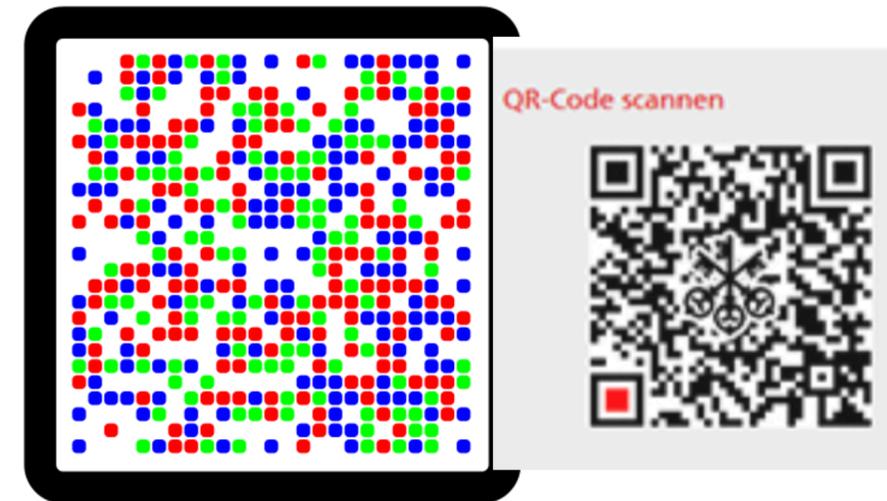
TAN Streich-Liste

TAN per SMS

TAN Generator

Photo TAN / QR TAN

Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN
1	165054	31	689033	61	225204	91	803264	121	999556	151	316455
2	845507	32	146500	62	909462	92	371251	122	194743	152	391789
3	688850	33	507008	63	001353	93	174368	123	690601	153	063157
4	506509	34	806187	64	969211	94	255887	124	267638	154	998327
5	463462	35	570685	65	507175	95	698961	125	125785	155	069997
6	972181	36	178959	66	954827	96	912793	126	947126	156	173673
7	510260	37	511061	67	868043	97	346694	127	561607	157	510386
8	811245	38	142901	68	449222	98	504109	128	835859	158	847480
9	528041	39	944010	69	612733	99	178873	129	667644	159	844433
10	356200	40	862795	70	877681	100	186211	130	991782	160	564911
11	469504	41	905695	71	190585	101	252128	131	150781	161	046297
12	149190	42	540713	72	813689	102	018525	132	388425	162	015563
13	235634	43	120133	73	538729	103	107691	133	327464	163	999999
14	271472	44	500192	74	660682	104	427044	134	789149	164	212198
15	043534	45	994692	75	591211	105	072846	135	930429	165	377554



Beispiel Postfinance 1

PostFinance

Hilfe und Support ▾

🔒 Login

E-Finance-Nummer / Benutzername

Passwort

[Passwort vergessen / ändern >](#)

Falls vorhanden:

Benutzeridentifikation

Weiter

Benötigen Sie Hilfe?

[Chat mit dem digitalen Assistenten >](#)

[Schritt-für-Schritt erklärt >](#)

E-Finance testen

[Demoversion E-Finance >](#)

Sie haben noch kein E-Finance?

[E-Finance bestellen >](#)

1. Faktor E-Finance-Nummer und Passwort

Aktionen:

**-E-Finance-Nummer und
Passwort bei E-Finance
eingeben.**

**Einmaliger Code für Eingabe
ins Kartenlesegerät wird
generiert.**

Beispiel Postfinance 2



2. Faktor

Kartenlesegerät und
Postfinance Karte und
PIN der Postfinance Karte

Aktionen

- Code aus Stufe 1 (Faktor 1) eingeben
- PIN für Postfinance Karte eingeben

Falls beide richtig sind, wird der Einmal
Code (TAN) für die Eingabe in E-Finance
generiert

Beispiel Postfinance 3



Eingabe für Kartenlesegerät

23 139 075

Code von Kartenlesegerät
467583211

1

2

Abbrechen

Login

Login abschliessen

TAN eingeben in E-Finance

Aktionen

- Einmal Code (TAN) in E-Finance eingeben
- Login klicken

Beispiel Kantonalbank 1

 [Hilfe](#)

Login eBanking 1 Vertragsnummer & Passwort > 2 Legitimation > 3 Startseite

Geben Sie Ihre Vertragsnummer und Ihr Passwort ein

Vertragsnummer

Passwort [Passwort vergessen?](#)

Sprache Deutsch [switch to English](#)

[Weiter >](#) [Abbrechen](#)

Probleme beim Login?
eBanking Support
Telefon 0844 840 140

Servicezeiten
Montag - Freitag
08:00 - 22:00
Samstag - Sonntag
09:00 - 18:00

Sie nutzen unser eBanking noch nicht?

- Sicherer Zugriff auf Ihre Bankgeschäfte jederzeit und von überall her
- Einfach Zahlungen erfassen
- Börsenkurse in Echtzeit abfragen und an der Börse handeln

[Jetzt kennenlernen](#)

1. Faktor Vertrags-Nummer und Passwort

Aktionen:

- Vertrags-Nummer und
Passwort bei ZKB eBanking
eingeben.
- Weiter klicken

Photo TAN wird generiert

Beispiel Kantonalbank 2

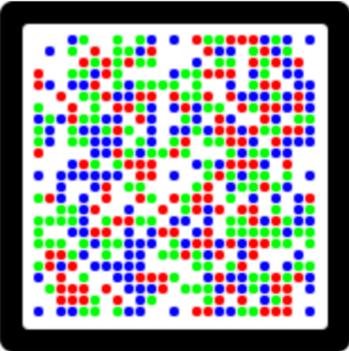
 Zürcher Kantonalbank

Hilfe [Logout](#)

Login eBanking ① Vertragsnummer & Passwort > ② Legitimation > ③ Startseite

Scannen Sie die Grafik

1. photoTAN Grafik Scannen Sie die untenstehende Grafik mit Ihrer App oder mit Ihrem Lesegerät.



2. TAN Geben Sie die angezeigte TAN ein.

Ihr letztes Login Donnerstag, 05. Dezember 2019 um 17:12 via eBanking

[Weiter >](#) [Abbrechen](#)

Bestätigung mit TAN
Wird Ihnen die TAN nicht angezeigt?

Prüfen Sie ob

- Sie die automatische Scharfstellung Ihrer Kamera aktiviert haben
- Sie gute Lichtverhältnisse haben
- die Kameralinse nicht verschmutzt ist

Scannen Sie die Grafik erneut.

eBanking Support
Telefon 0844 844 848

Servicezeiten
Montag - Freitag
08:00 - 22:00
Samstag - Sonntag
09:00 - 18:00

2. Faktor

- Photo TAN (Einmal Code)
- Smartphone mit ZKB App oder ZKB Photo TAN Gerät

Aktionen:

- Photo TAN aus der APP oder vom Photo TAN Gerät eingeben im TAN Feld
- Weiter klicken

Gratuliere, Sie sind im Banking

Pause

Bezahlen mit Kreditkarte

- Kreditkarten
- Prepaid Karten
- Debitkarten
- Sorgfaltspflichten
- Wie funktioniert Kontaktloses Bezahlen

Sorgfaltspflichten Kreditkarten

1. Unterschrift auf der Karte
2. Sichere Aufbewahrung
3. Verlust, Diebstahl und Kartenmissbrauch sofort melden
4. Geheimhaltung PIN Code
5. Prüfung der Monatsrechnung und Meldung von Missbrauch
6. Mitteilung von Änderungen
7. Zahlungstransaktionen im Internet mit bestmöglicher Sicherheit

Wie funktioniert Kontaktloses Bezahlen



Kontaktloses Bezahlen bezeichnet eine Zahlungsfunktion, bei der Zahlungen berührungslos z.B. über Near Field Communication (NFC) abgewickelt werden. Kontaktloses Bezahlen wird heutzutage von den meisten Zahlungskarten und aktuellen Smartphones sowie POS-Terminals unterstützt.

Die Übertragungreichweite eines solchen NFC-Chips ist in der Regel auf maximal vier Zentimeter begrenzt, in der Praxis funktioniert die NFC-Zahlung häufig nur bis zu einem Abstand von einem Zentimeter.

Bei einer Transaktion mittels NFC werden die Kartenummer, das Gültigkeitsdatum sowie der Betrag übertragen.[4] Die Übertragung wird in der Regel durch einen Piepton bestätigt.

Der Höchstbetrag für kontaktlose Zahlungen ohne Eingabe der PIN liegt in der Schweiz standardmässig bei CHF 39.99 pro Transaktion. Ab CHF 40 oder nach 4 Transaktionen in kurzer Zeit muss die PIN eingegeben werden.



Vorsicht beim kontaktlosen Bezahlen



1. Es ist vergleichsweise einfach mit der entsprechenden technischen Ausrüstung die Kreditkartendaten einer Person herauszufinden, indem man die Daten über den Funkchip der Karte herausliest. Mit den erbeuteten Daten können Kriminelle beispielsweise bei Anbietern online einkaufen, welche die dreistellige Sicherheitsnummer auf der Karte nicht verlangen (beispielsweise bei Amazon) und so einen finanziellen Schaden verursachen.
2. Mit einem mobilen Bezahlterminal können Betrüger genügend nahe an die Kreditkarte einer Person gelangen und so weniger als CHF 40 ohne Kenntnis der Person abbuchen. Vor allem im Ausland gefährlich, da in CH Registrierungspflicht.
3. Mit einer gestohlenen Karte können 4x Beträge kleiner als CHF 40 abgehoben werden ohne PIN.

Schutzmassnahmen

1. **Funkchip deaktivieren, geht bei Postfinance Card, nicht bei Kreditkarten**
2. **Schutzhülle aus Metall verwenden, z.B. Alufolie, käufliche Kartenschutzhüllen**

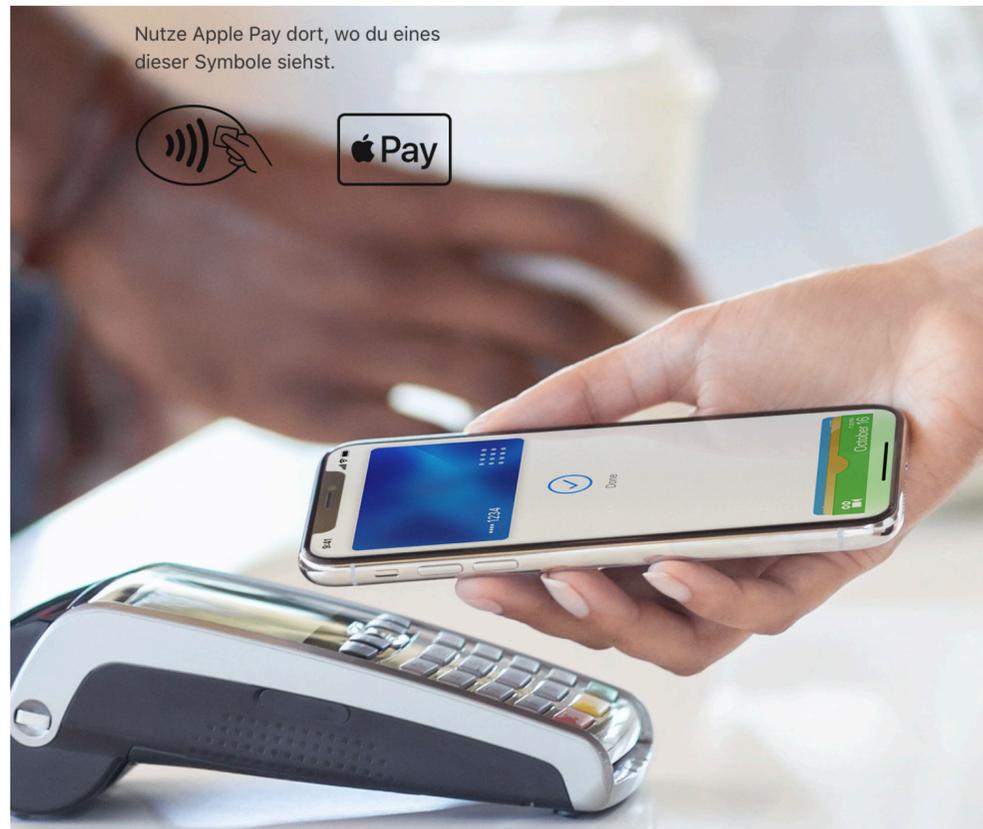
Bezahlen mit dem Handy

Apple Pay, Samsung Pay, Google Pay, TWINT, PayPal

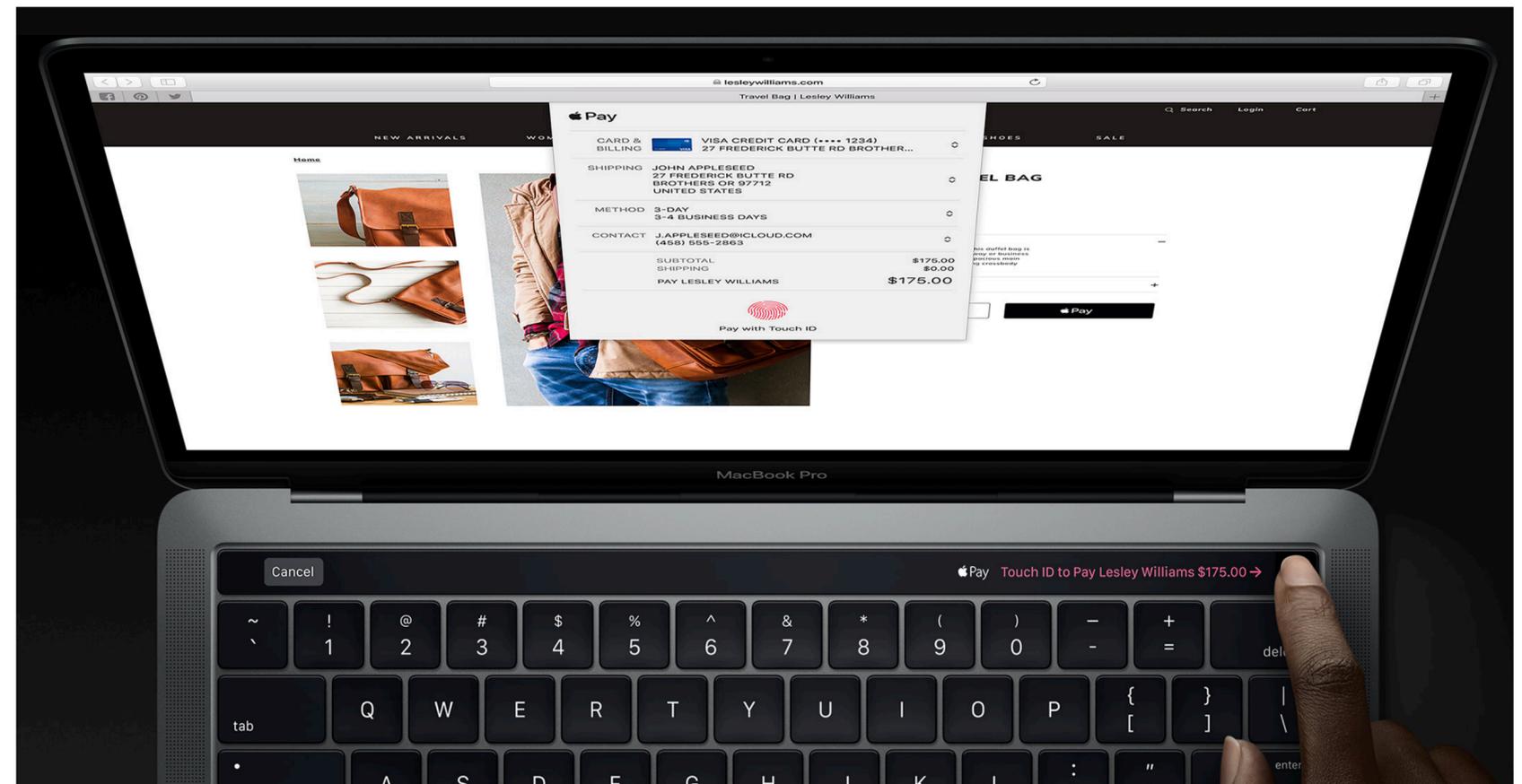
- Sicher, weil das Smartphone (oder Smartwatch) geschützt ist durch biometrische Daten, Fingerabdruck oder Gesichtserkennung
- Komfortabel, weil du deinen Fingerabdruck und dein Gesicht immer dabei hast
- Biometrische Daten sind sehr sicher

Apple Pay

Im Geschäft bezahlen



Im Web bezahlen



Datenschutz und Sicherheit. Bei jeder einzelnen Zahlung.

Weitere Informationen: <https://www.apple.com/chde/apple-pay/>

Samsung Pay

Im Geschäft bezahlen

Schnell und sicher

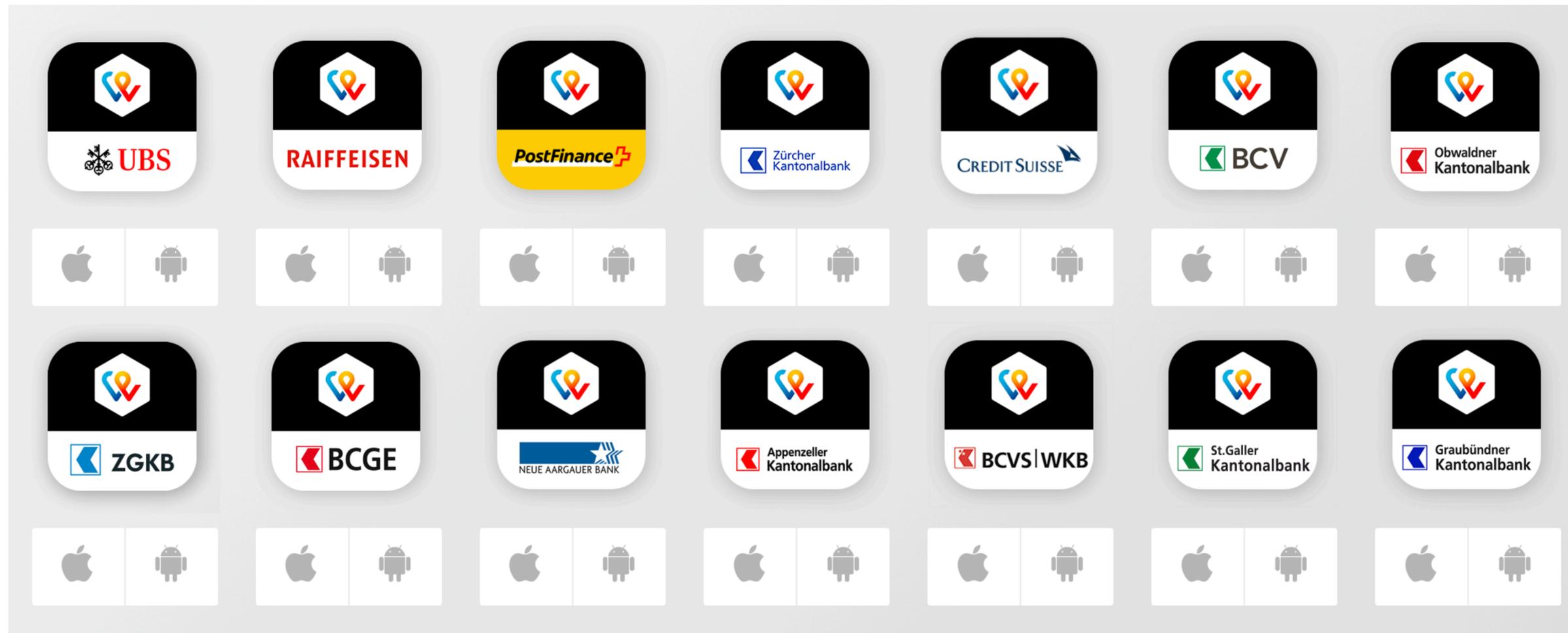


Datenschutz und Sicherheit. Bei jeder einzelnen Zahlung.

Weitere Informationen: <https://www.samsung.com/ch/samsung-pay/>

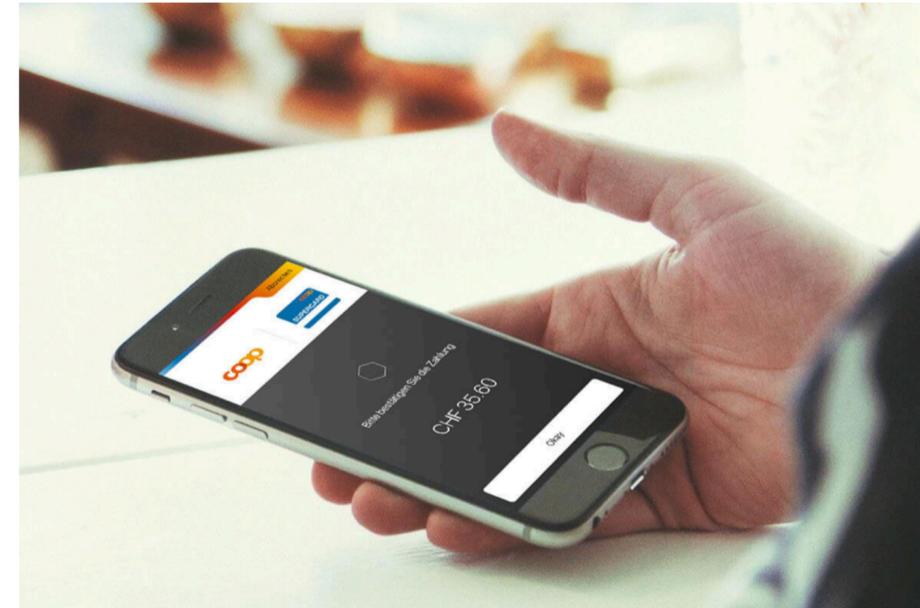
TWINT

TWINT ist die App der Schweizer Banken zum Bezahlen und „Geld senden und anfordern“ direkt unter Benutzern. Die Identifikation ist Ihre **Mobiltelefonnummer**. Sie benötigen die App Ihrer Bank und verknüpfen Ihr Konto mit der App. Sie bezahlen Online, an der Kasse, am Automaten, auf dem Parkplatz



Weitere Informationen: <https://www.twint.ch>

TWINT



Weitere Informationen: <https://www.twint.ch>



PayPal ist ein Online Bezahldienst mit Sitz in San José, Kalifornien. 1,1 Million aktive Kunden nutzen PayPal allein in der Schweiz, 246 Millionen weltweit.

Das PayPal-Konto ist ein virtuelles Konto: Die Identität des Kontos wird durch die **E-Mail-Adresse** des PayPal-Mitglieds definiert, es gibt also keine Kontonummer. Mit dem Konto können Zahlungen an Dritte ausgeführt und Zahlungen von Dritten empfangen werden. Dabei fungiert PayPal als Dienstleister für den Transfer. PayPal übernimmt nicht die Funktion eines Treuhänders, das heisst, es wird lediglich die Zahlungsabwicklung übernommen, unabhängig von der Leistungserbringung durch den Verkäufer.

Bei PayPal kann man ein Bankkonto oder eine Kreditkarte anbinden oder Geld auf das Konto laden für die Bezahlung.

Weitere Informationen: [Paypal](#)

ParkingPay

Wie funktioniert die App?



Strassenparkplätze



mit Badge

Parkhäuser



Bewilligungen

Parkplätze und Parkzonen in Wallisellen sind abgedeckt

Strassenparkplätze



Wie funktioniert's?

1. Auto parkieren, Parkingpay-App öffnen und Zone wählen.
2. Voraussichtliche Parkdauer einstellen und Parkvorgang starten.
3. Wenn zurück im Auto, Parkvorgang stoppen.

Vorteile

- Bargeldlos bezahlen
- Nur effektive Parkdauer bezahlt
- Kein Gang zur Parkuhr

Bewilligungen



Wie funktioniert's?

1. Wenn nötig, Freigabe zum Kauf der Bewilligung beantragen.
2. App öffnen oder im Browser parkingpay.ch öffnen und Bewilligung kaufen.
3. Ein paar Tage vor Ablauf kriegen Sie ein Erinnerungsmail. Die Bewilligung kann bequem mit Parkingpay verlängert werden.

Vorteile

- Kein Gang zur Gemeinde
- Bargeldlos
- Keine Karte hinter der Windschutzscheibe

Fragen zum bezahlen?

Aktuell

Anmelden zum Support

Wie auf Einladung antworten?

Rolf

Windows 7 Ende Support

Was ist zu tun?

Markus

iOS 13 Update

Wie updaten?

Rolf

macOS Catalina Update

Wie updaten?

Rolf

Android Update

Wie updaten?

Rolf

Bei allen Softwareupdates

Immer zuerst ein Backup

Markus und Rolf

Der Support für Windows 7 endet am 14. Januar 2020

Technische Unterstützung und Software-Updates von Windows Update, die zum Schutz Ihres PCs beitragen, sind für das Produkt nicht mehr verfügbar. Microsoft empfiehlt dringend, auf Windows 10 umzusteigen, um zu vermeiden, dass Sie einen Service oder Support benötigen, der nicht mehr verfügbar ist.

[Was bedeutet der Ablauf des Supports für mich?](#)

Was kann ich tun?

Ist für meinen PC ein Upgrade auf Windows 10 möglich und sinnvoll?

Wie führe ich ein kostenloses Upgrade auf Windows 10 durch? 1)

Was geschieht, wenn ich weiterhin Windows 7 verwende?

Kann Windows 7 nach dem 14. Januar 2020 weiterhin aktiviert werden?

Wird Internet Explorer weiterhin unter Windows 7 unterstützt?

Wird Microsoft Security Essentials meinen PC nach Ablauf des Supports weiterhin schützen?

Kann ich meine vorhandenen Programme auf einen neuen Windows 10-PC verschieben?

Wie wirkt sich der Ablauf des Supports von Windows 7 auf meine Microsoft Office-Apps aus?

1) Tipps im Support erhältlich

iOS 13 und iPadOS 13

Informationen zu iOS 13

Neue Features in iOS 13

Wie updaten?

iOS 13 ist kompatibel mit

iPhone 11

iPhone 11 Pro

iPhone 11 Pro Max

iPhone XS

iPhone XS Max

iPhone XR

iPhone X

iPhone 8 / Plus

iPhone 7 / Plus

iPhone 6s / Plus

iPhone SE

iPod touch (7. Generation)

Informationen zu iPadOS 13

Neue Features in iPadOS 13

Wie updaten?

iPadOS 13 ist kompatibel mit

12,9" iPad Pro

11" iPad Pro

10,5" iPad Pro

9,7" iPad Pro

iPad (7. Generation)

iPad (6. Generation)

iPad (5. Generation)

iPad mini (5. Generation)

iPad mini 4

iPad Air (3. Generation)

iPad Air 2

macOS Catalina

Überblick

Neue Features

Wie upgraden?

Für Informationen zu deinem Mac Modell klickst du auf das Apple Symbol oben links auf dem Bildschirm und wählst «Über diesen Mac». Diese Mac Modelle sind kompatibel mit macOS Catalina:

MacBook (Anfang 2015 oder neuer)

MacBook Air (Mitte 2012 oder neuer)

MacBook Pro (Mitte 2012 oder neuer)

Mac mini (Ende 2012 oder neuer)

iMac (Ende 2012 oder neuer)

iMac Pro (2017)

Mac Pro (Ende 2013 oder neuer)

Android

Kein einheitliches Vorgehen

Zeitpunkt und Version hängt vom Hersteller ab

Wichtig: Immer die angebotenen Sicherheitsupdates installieren.

Bei den meisten Herstellern zu finden unter:

Einstellungen/System/Softwareaktualisierung

**Nächster Computeria Support
Mittwoch, 12. Februar 2020
Alterszentrum Wägelwiesen**

Einladung folgt

Infos und Anmeldung unter:

www.computeria-wallisellen.ch/support

Nächster Computeria Treff
Mittwoch, 19. Februar 2020
Alterszentrum Wägelwiesen, Mehrzwecksaal

Thema: Passwortverwaltung

Danke