Sicherheit beim Online-Banking

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

So schützen Sie sich vor Trickbetrügern

Eine Veranstaltung der Digital-Botschafter:innen der Verbandsgemeinde Gau-Algesheim

Was ist Online-Banking?

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Abwicklung von Bankgeschäften über das Internet

Den Kontostand abfragen, eine Überweisung absenden oder einen Dauerauftrag einrichten – alles per Mausklick bequem von Ihrem PC aus. Einmal eingerichtet haben Sie die Wahl, ob Sie Ihr Bankgeschäft vom Computer aus erledigen, oder doch Ihre Vertrauensperson vor Ort aufsuchen – sofern eine Bankfiliale noch vorhanden ist.

Voraussetzungen:

- Gerät mit Internetzugang (Smartphone, Tablet, PC)
- Bankkonto
- Zugangsdaten für das Online-Banking
- Vertrauen in die Sicherheitsmaßnahmen der Bank

Was ist Online-Banking?

Bankgeschäfte per Mausklick erledigen

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Vorteile:

+ Durchführung von Bankgeschäften bequem von zu Hause
+ Unabhängig von den Öffnungszeiten und Erreichbarkeit Ihrer Filiale
+ Überblick über Ihre gesamten Kontoumsätze
+ Kostenersparnis

So können Sie Ihre Bankgeschäfte sowohl von zu Hause z.B. von Ihrem PC mit einem Browser oder auch von unterwegs aus erledigen. Für das mobile Banking brauchen Sie das entsprechende Programm (App) auf Ihrem Smartphone.

Wie komme ich zum Online-Banking?

Jede Bank hat ihren eigenen Weg, wie Sie zum Online-Banking kommen und nutzen können.
Einige Banken bieten Demoseiten zu ihrem Online-Banking Angebot an. Hier können Sie z.B. testweise eine Überweisung eingeben und die verfügbaren Online-Services kennenlernen.

Ihre Zugangsdaten zum Online-Banking können Sie bei Ihrer Hausbank anfordern, entweder direkt in der Filiale oder über die Webseite Ihrer Bank. Sobald Sie Ihre Zugangsdaten haben, können Sie die Internetseite Ihrer Bank aufrufen und sich mit Ihrem Benutzernamen (Benutzernummer) und Passwort (PIN) anmelden.

Schritt für Schritt zum Onlinebanking

Zugangsdaten bei der Bank beantragen

TAN-Verfahren wählen

Bedingungen der Bank lesen

Bankgeschäfte online erledigen

Video zu einem Betrugsfall beim Online-Banking

Quelle: https://www.ardmediathek.de/video/marktcheck/mobiles-bezahlen-mit-dem-smartphone-wie-sicher-ist-apple-pay/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzE3Njg3MzA (SWR Marktcheck, 29.11.2022, 8:38 min.)

Wie kam es zu diesem Betrug? Was ist hier schiefgelaufen?

Fehler Nr. 1:

Zunächst wurden die Bankdaten des Kunden mittels einer sogenannten Phishing-Mail von dem Betrüger in Erfahrung gebracht.

Wie funktioniert eine Phishing-Mail?

Beim Phishing geht es darum, mit gefälschten E-Mails und anderen Nachrichtenformen an Daten von Nutzer*innen zu kommen. Dabei werden Nutzer*innen auf gefälschte Websites gelockt, um dort ihre Daten preiszugeben.

Beispielsweise erhält man eine E-Mail, in der man dazu aufgefordert wird, die eigenen Bankdaten auf einer Website anzugeben. Die entsprechende Seite sieht der Originalseite der Bank sehr ähnlich, ist allerdings eine Betrugsseite.

Der Begriff „Phishing" setzt sich zusammen aus den Wörtern „fishing" (zu Deutsch „angeln") und „Passwort". Phishing ist also das Angeln nach Passwörtern.

Wie erkenne ich eine Phishing-Mail?

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Vorsicht, Phishing! Betrügerische E-Mails erkennen

Gefälschte Absender-Adresse
Ist die E-Mail-Adresse des Absenders z.B. durch einen Vergleich zu verifizieren? Kann der Absender den Versand der Mail persönlich/ telefonisch bestätigen?

Abfrage vertraulicher Daten
Fordert die E-Mail zur Eingabe persönlicher Informationen auf? Werden Geheimnummern oder Passwörter abgefragt?

Vorgetäuschter dringender Handlungsbedarf
Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf? Wird eine Nachricht des Absenders erwartet?

Links zu gefälschten Webseiten
Enthält die E-Mail Verlinkungen, die auf andere Webseiten verweisen? Welche Ziel-URL wird bei einem Mouseover angezeigt?

Sprachliche Ungenauigkeiten
Ist die Anrede unpersönlich formuliert? Enthält der Text Rechtschreib- oder Zeichenfehler?

www.bsi-fuer-buerger.de

Wie kann ich das verhindern?

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Halten Sie Ihre Zugangsdaten stets geheim.

Benutzername, Passwort, PIN und TAN sollten niemandem verraten werden. Außerdem sollte man nie der Aufforderung in E-Mails folgen, solche Daten preiszugeben.

Eine Bank wird **niemals** die Angabe von PINs oder TANs zu Kontrollzwecken per E-Mail oder Telefon verlangen – dabei handelt es sich mit großer Wahrscheinlichkeit um Betrugsversuche.

Lassen Sie sich nicht von vermeintlichen Links täuschen.

Die Internetadresse zur Bank sollte man immer selbst eingeben und dann unter den Favoriten im Browser speichern.

Nur über diesen Weg bei der Bank einloggen!!!

Hinweise auf Betrug

Bei E-Mails und Websites deuten **Rechtschreibfehler**,
eine falsche Internetadresse oder ein fehlendes Schlüsselsymbol in der Statusleiste auf Fälschungen hin. Zum Schutz vor Phishing sollte man darauf immer zusätzlich achten.

Nutzen Sie Onlinebanking nur in **sicherer Umgebung**. Öffentliche Computer und Netzwerke sind nicht der richtige Ort für Bankgeschäfte. Aber auch auf dem heimischen Rechner sollte man Zugangsdaten zum Onlinebanking nicht ungesichert speichern, sondern immer wieder neu eingeben.

Behalten Sie Ihre **Konten** im Blick.
Prüfen Sie daher regelmäßig Ihre Kontobewegungen. Bei Verfügungen, die man nicht selbst veranlasst hat, sollte man sich sofort an die Bank wenden und eventuell Anzeige bei der Polizei erstatten.

Zwei-Faktor-Authentifizierung

Fehler Nr. 2:

Fehlende **Zwei-Faktor-Authentifizierung**.
In unserem Film wurde auf diese verzichtet. Wieso die Bank nicht darauf bestanden hat, ist rätselhaft.

Was ist das?

Die **Zwei-Faktor-Authentifizierung**, häufig auch **Zwei-Faktor-Authentisierung** genannt, bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).
Typische Beispiele sind Bankkarte und PIN beim Geldautomaten, Fingerabdruck und Zugangscode in Gebäuden, oder Passwort und Transaktionsnummer (TAN) beim Online-Banking.

Zwei-Faktor-Authentifizierung

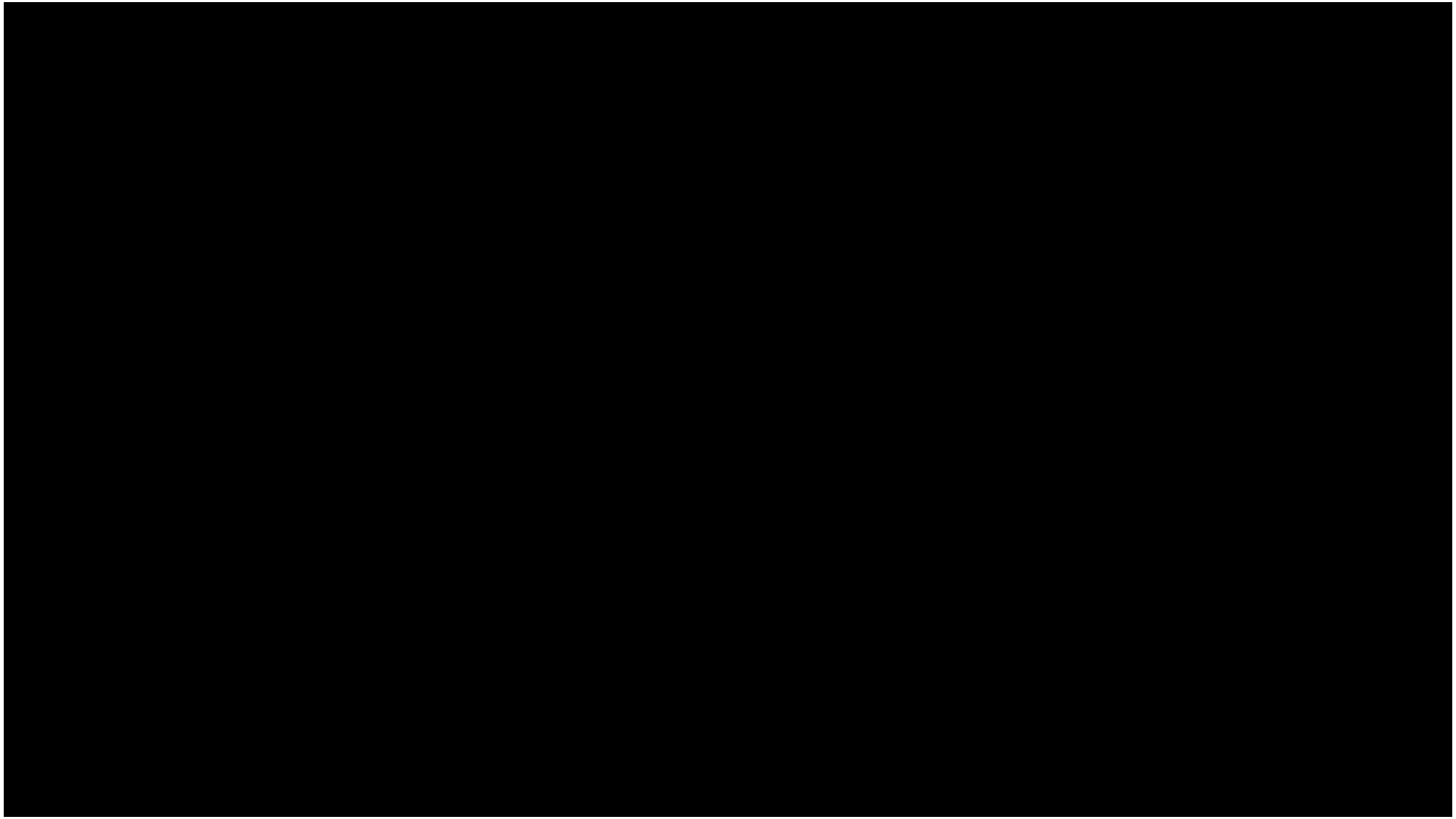
Wissen	Besitz	Sein / Inhärenz

Beispiel:

Die einfachste Zwei-Faktor-Authentifizierung

verbraucherzentrale
Rheinland-Pfalz

Video zu TAN-Verfahren beim Online-Banking



Quelle: https://www.youtube.com/watch?v=8_AXxmqawOI (Verbraucherzentrale Nordrhein-Westfalen, 2018, 2:39 min.)

smsTAN wird abgeschafft?

Beim smsTAN Verfahren wird an die hinterlegte Mobilnummer (daher auch mTAN oder mobileTAN genannt) eine SMS mit der TAN gesendet. Diese Methode gilt als angreifbar.

Alternativen:

- TAN über eine Smartphone-App: pushTAN, appTAN, photoTAN
- TAN-Generatoren (z.B. mit girocard):
  eine Grafik wird auf dem PC erzeugt und über das Lesegerät mit Bankkarte ausgelesen. Die auf dem Gerät gezeigte TAN wird dann am PC eingegeben. Mittlerweile gibt es auch Smartphone Apps, die diese Bilder am PC auslesen können und die TAN erzeugen.
  chipTAN, smartTAN, photoTAN, QR-TAN

Es sollte immer das TAN-Verfahren genutzt werden, das die Banken selbst für ihre Kunden festlegen.

smsTAN wird abgeschafft?

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Die meisten Banken bieten Apps für mobile Endgeräte an, sodass **pushTAN** weit verbreitet ist. Für Bankkundinnen und -kunden bietet das Verfahren, bei richtiger Anwendung, ein gutes Sicherheitsniveau. Für die Banken entstehen mit pushTAN die geringsten Kosten.

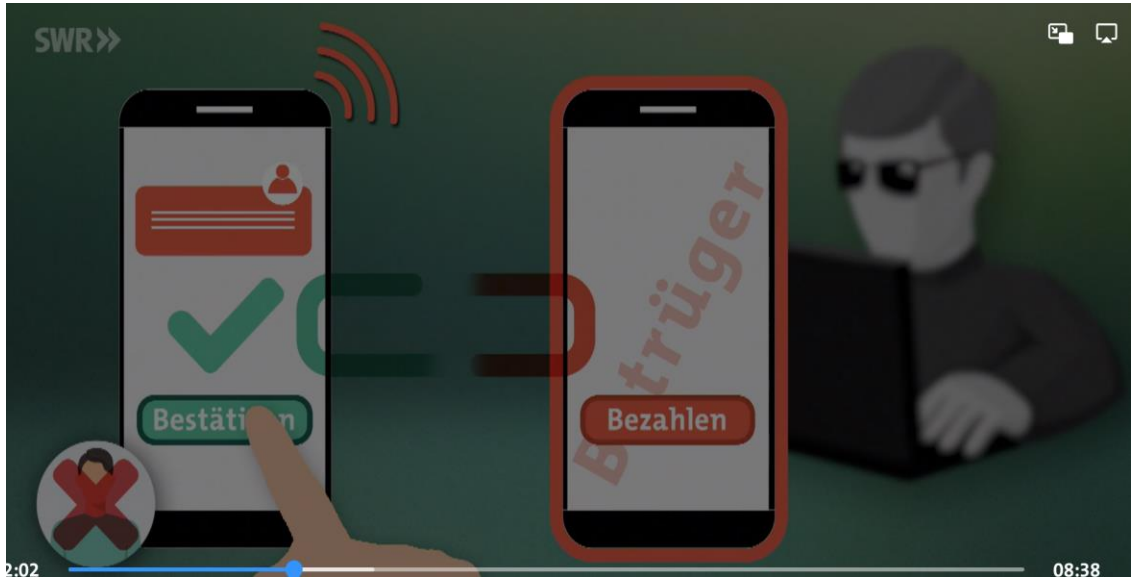
Mit der **PhotoTAN**, bei der die Daten für die Erzeugung der TAN auf einem anderen Gerät erzeugt werden, steht ein weiteres sicheres Verfahren zur Verfügung.

Jedoch bleibt der Einsatz eines externen **TAN-Generator** am sichersten, da dieser vom Internet getrennt ist und ausschließlich für das Onlinebanking benutzt wird.

Generell sind die in Deutschland angewendeten Versionen der TAN-Generierung sicher, solange die Nutzerinnen und Nutzer Banking und TAN-Erstellung immer auf **unterschiedlichen Geräten** durchführen.

Quelle: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/smsTAN/sms-tan_node.html

Fehler Nr. 3:



Der Betroffene lässt sich durch eine fingierte Mail und einen Anruf der Betrüger dazu verleiten, das eigene Konto für das Handy der Betrüger freizuschalten und somit freien Zugang für andere Bezahlsysteme zu gewährleisten!

Fehler Nr. 4:

Der Betroffene verlässt sich darauf, dass der Bank schon das häufige Abheben auffällt und sie darauf reagieren.

Ein fataler Fehler, wie sich herausstellt.

Fehler Nr. 5:

Der Betroffene hat sein Konto offensichtlich nicht öfter kontrolliert. Hätte er dies getan, hätten ihm die ungewöhnlichen Kontobewegungen auffallen müssen!

Fehler Nr. 6:

Für das Bankkonto wurde bei den Einstellungen **kein Limit** bzw. Maximalbetrag für Überweisungen pro Tag/Woche festgelegt.

Durch die Einrichtung eines Tages- und eines Wochenlimits kann der Schaden zumindest begrenzt werden.

Auf welche Anzeichen für Betrugsversuche sollte ich achten?

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

Kommt Ihnen etwas im Zusammenhang mit dem Onlinebanking „komisch" vor, sollten Sie den Vorgang sofort abbrechen. Achten Sie vor allem auf die folgenden Warnsignale:

- **Schlechte Rechtschreibung:** Schreibfehler, aber auch ungewöhnliche Satzkonstruktionen oder englische Begriffe weisen darauf hin, dass eine Mail oder Webseite nicht von der Bank stammt. Aber die Qualität wird immer besser, sodass auch auf den ersten Blick fehlerfreie Seiten betrügerisch sein können.
- **Schlampiges Design:** Verschobene Formularfelder oder Grafikfehler? Dann handelt es sich wahrscheinlich um einen Betrugsversuch.
- **Login-Bitten:** Ihre Bank wird Sie niemals in E-Mails auffordern, sich einzuloggen, indem Sie auf einen Link klicken sollen.
- **Anhänge in E-Mails:** Keine Bank verschickt E-Mails mit Anhängen. Wenn Sie diese öffnen, riskieren Sie, sich Schadsoftware einzufangen. Jede Datei kann verseucht sein, auch Bilder oder PDF-Dateien.

Anzeichen für Betrugsversuche

DIGITAL BOTSCHAFTERINNEN & BOTSCHAFTER RHEINLAND-PFALZ

- **Schloss-Symbol im Browser:** Webseiten von Banken nutzen eine SSL-Verschlüsselung. Diese können Sie in Ihrem Browser an dem Schloss in der Adresszeile erkennen; die Webadresse beginnt mit „**https**://“.
  Webadressen, denen nur „http://“ voransteht, sollten Sie misstrauisch machen.
- **Anrufe von der Bank:** Wenn Sie angerufen werden und vermeintliche Bankmitarbeiter:innen etwas von Ihnen wollen, sei es auch nur das Geburtsdatum oder dass Sie eine Nummer vorlesen sollen, beenden Sie das Gespräch und rufen Sie selbst die Nummer Ihrer Bank an. Ihre Bank wird Sie niemals nach TANs fragen.
- **Unaufgeforderte SMS mit Links:** Wenn Sie eine SMS mit einem Link bekommen, sollten Sie diesen nicht anklicken, erst Recht nicht, wenn Sie nicht bewusst einen Vorgang im Onlinebanking ausgelöst haben.

Generell gilt: Es gibt keinen Grund, sich von vermeintlichen Mitarbeiter:innen unter Druck setzen zu lassen. Bei einer angeblichen Änderung des TAN-Verfahrens, einer Sicherheitslücke oder Schadensfällen wird Sie Ihre Bank nicht anrufen, um in einem Telefonat mit Ihnen sicherheitsrelevante Umstände zu ändern.

Betrügerische E-Mails behandeln zumeist Themen, die verunsichern, wie z.B. Kontosperrungen, angeblichen Identitätsklau, Änderungen im Onlinebanking, Datenabgleich oder Ähnliches. Sie können solche E-Mails von Ihrer Bank allenfalls lesen. Sie sollten aber **niemals** auf Links klicken oder Anhänge öffnen.

Tipps für sicheres Online-Banking

Die Banken setzen eine Reihe an Sicherheitsmaßnahmen ein, damit Sie Ihre Bankgeschäfte im Internet **sicher** durchführen können. Sie selbst können allerdings auch einen wesentlichen Beitrag dazu leisten:

- Achten Sie darauf, dass auf Ihrem Gerät stets die aktuelle Version des **Betriebssystems** und des **Browsers** verwendet wird, **Virenscanner** und **Firewalls** installiert sowie Sicherheitsupdates vorgenommen sind.
- Rufen Sie die Website Ihrer Bank durch Eintippen der Internetadresse in Ihrem Browser auf. So verhindern Sie, dass Sie irrtümlich gefälschten Links folgen.

Mehr Tipps …

- Kontrollieren Sie, ob das Sicherheitsschloss im Browser geschlossen ist.
- Vermeiden Sie Online-Banking in fremden oder öffentlichen WLAN-Netzen.
- Schützen Sie Ihre persönlichen Zugangsdaten (Nutzerkennung, Kontonummer, PIN, TAN, Benutzername/Passwort usw.) und halten Sie diese geheim.
- Melden Sie sich immer ab (Logout).
- Klicken Sie keine Links in verdächtigen E-Mails an. Ihre Bank fordert Sie NIE per E-Mail oder telefonisch auf, Ihre Zugangsdaten oder vermeintliche Sicherheitscodes bekannt zu geben! Im Zweifelsfall kontaktieren Sie direkt Ihre Ansprechperson bei der Bank.

Und zu guter Letzt:

Immer Handy, Tablet, Laptop und Computer aktuell halten!

Das heißt: alle angebotenen Updates durchführen und ab und zu selbst kontrollieren, ob es neue Updates gibt.

DANKE für Ihre Aufmerksamkeit!