bankenverband

fokus | verbraucher

Online- und Mobile-Banking – sicher über Browser und App

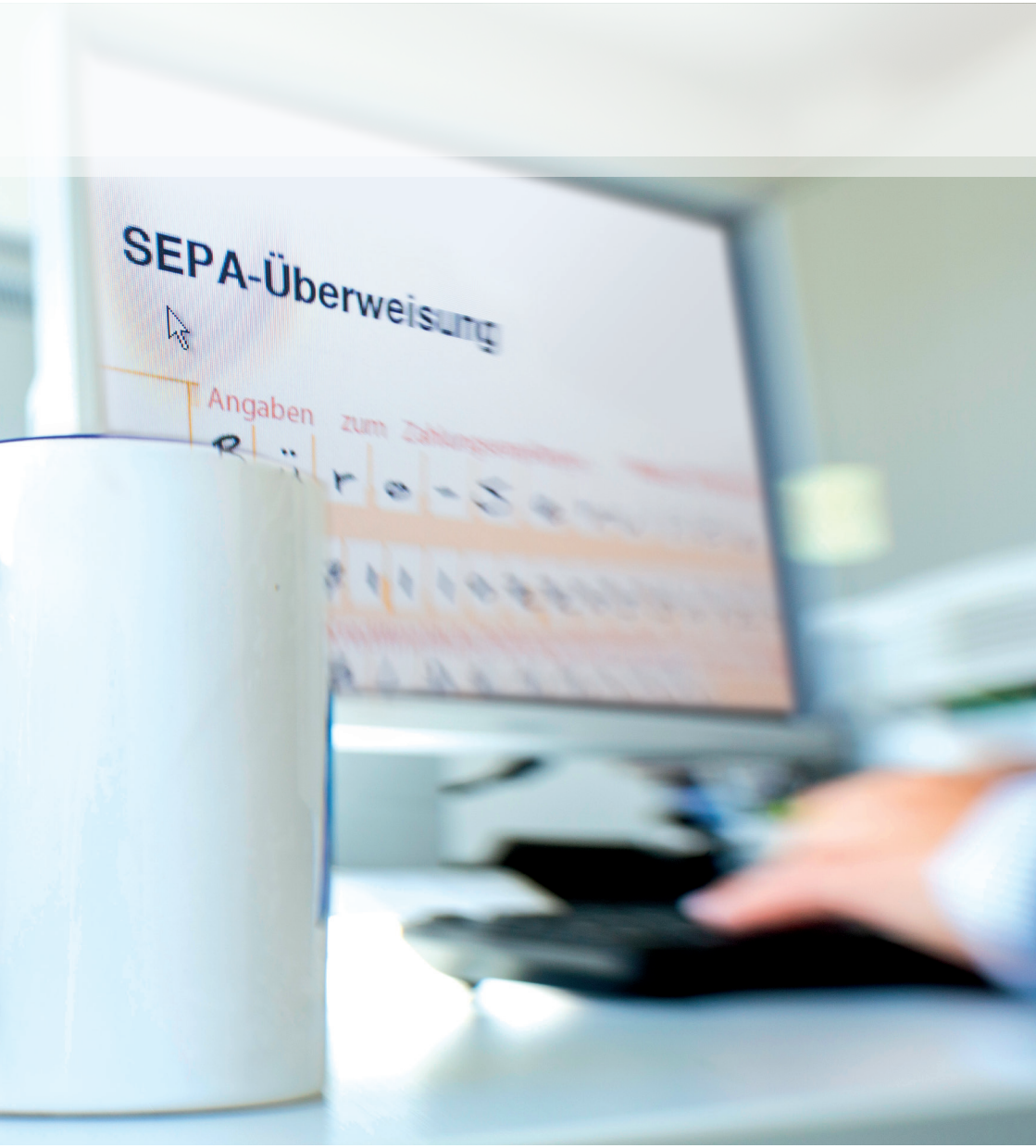
Eine Information der privaten Banken

Berlin, November 2016

Online- und Mobile-Banking – sicher über Browser und App

Informationen für Privatkunden

Berlin, November 2016


SEPA-Überweisung
Angaben

Inhalt

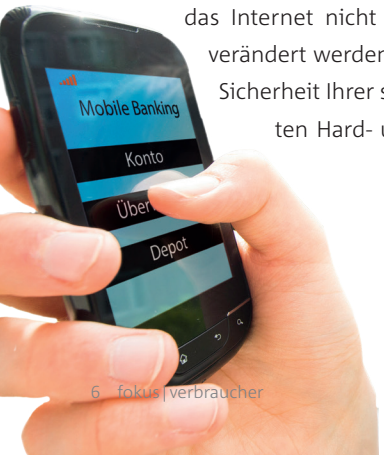
1

Bequem und sicher über Browser und App

Bankgeschäfte über das Internet abzuwickeln, ist schnell, einfach und bequem. Viele Menschen nutzen das Online-Angebot ihrer Bank, um von zu Hause oder unterwegs „die eigene Bankfiliale zu besuchen“ – und das rund um die Uhr. Online-Banking kann über Browser oder App auf Geräten wie PC, Smartphone, Tablet oder auch moderne Fernseher (Smart-TV) genutzt werden. Überweisungsaufträge, Wertpapierhandel, Kreditanträge, Sparanlagen sowie der Abruf aktueller Kontoinformationen können so unabhängig von den Öffnungszeiten der Bank erledigt werden.

Ihre „persönliche Bankfiliale“ im Online- und Mobile-Banking können Sie sicher besuchen, wenn Sie sich an bestimmte „Spielregeln“ und Tipps halten.

Ihre Bank führt umfangreiche Maßnahmen zur Absicherung ihrer Online-Angebote durch. Diese gewährleisten unter anderem, dass Ihre vertraulichen Daten bei der Übertragung über das Internet nicht eingesehen und verändert werden können. Auf die Sicherheit Ihrer selbst ausgewählten Hard- und Software hat Ihre Bank jedoch keinen Einfluss. Damit die von Ihrer Bank vorgesehenen Sicherheitsvorkehrungen nicht durch Manipulationen aus dem Internet umgangen werden können, müssen auch Sie Vorkehrungen zum Schutz Ihres Gerätes treffen.



Nachfolgend zeigen wir Ihnen anhand von Beispielen, wie eine Online-Banking-Sitzung zur Ausführung einer Überweisung mit Hilfe eines Internetbrowsers sicher durchgeführt werden kann. Die Aussagen gelten sinngemäß auch für Online-Banking über andere Kanäle wie zum Beispiel per FinTS bzw. HBCI.

Zuallererst sollten Sie sich fragen, von welchem Gerät aus Sie Bankgeschäfte tätigen wollen. Am besten verwenden Sie Ihr eigenes Gerät. Wenn Sie das Gerät nicht kennen, wie zum Beispiel den PC in einem Internetcafé oder das Tablet eines Bekannten, dann wissen Sie natürlich auch nicht, welche Gefahren dort lauern. Schadsoftware könnte zum Beispiel alle Ihre Tastatur- und Mauseingaben sowie Bildschirminhalte unbemerkt mitschneiden, manipulieren und an Dritte weiterleiten.

2

Typische Gefahren: Phishing und Schadsoftware

Hinter Phishing verbirgt sich das Ausspähen von Zugangs- und Autorisierungsdaten mit Hilfe von täuschend echt aussehenden Internetseiten, falschen Namen oder Adressen zum Zweck des Betrugs. Als Schadsoftware (engl. Malware) werden Apps oder Computerprogramme wie zum Beispiel Computerviren und trojanische Pferde bezeichnet, die unerwünschte und ggf. schädliche Funktionen unbemerkt ausführen. Hierzu zählen beispielsweise das Ausspähen sensibler Daten, wie Passwörter oder Kontaktdaten, und das Weiterleiten dieser an den Betrüger sowie das Verfälschen von Transaktionsdaten. Damit die Schadsoftware nicht entdeckt wird, schaltet diese teilweise auch Sicherheitssoftware wie die Personal Firewall oder das Antivirenprogramm aus. Ein Angreifer kann auf derart infizierte Geräte zugreifen und die Fernkontrolle über alle Funktionen erlangen. Damit übernimmt der Angreifer Ihr Gerät, als säße er direkt davor oder hielte es in der Hand.

Wie können Sie erkennen, ob Ihr PC infiziert ist? Achten Sie auf ungewöhnliches Verhalten bei der Nutzung Ihres Gerätes: Ignorieren Sie niemals Meldungen des Betriebssystems, Ihrer Sicherheits- und Anwendungssoftware sowie Ihrer Apps! Einfaches Wegklicken oder unbedachtes Zustimmen kann schaden. Sobald für Ihren PC, Ihr Smartphone oder Tablet eine Softwareaktualisierung verfügbar ist, sollten Sie diese installieren. Je länger Sie wichtige Aktualisierungen hinauszögern, desto eher werden Sie für Betrüger angreifbar.

Wenn Sie eine Meldung nicht verstehen, sollten Sie dieser auf den Grund gehen. Holen Sie hierzu Informationen beispielsweise über eine Suchmaschine ein oder fragen Sie einen Fachmann.

Ist plötzlich das Antivirenprogramm oder eine andere Sicherheitssoftware nicht mehr aktiv, so ist das ein starkes Anzeichen dafür, dass ein Schadprogramm den jeweiligen Schutz manipuliert oder gar ausgeschaltet hat. Das Gleiche gilt auch für nicht funktionierende automatische Updates, zum Beispiel des Betriebssystems oder des Antivirenprogramms. Als Folge ist Ihr Gerät anfälliger und bei Angriffen weniger geschützt.

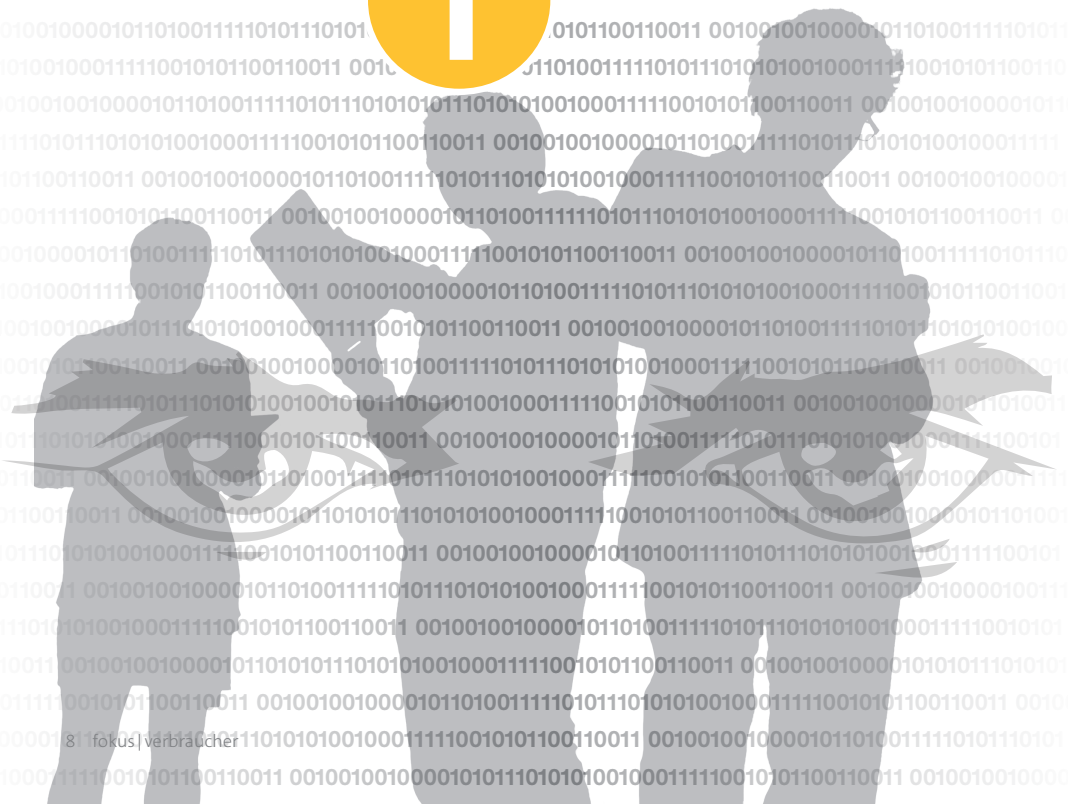
Arbeiten Sie am Computer nicht mit Administratorrechten oder mit Smartphones/Tablets, die gerootet oder gejailbreakt[1)] wurden. Erlangt ein Angreifer Zugriff auf Ihr Gerät, kann er so wichtige Sicherheitsfunktionen leichter umgehen. Insbesondere kann der Angreifer dann

1) Nicht autorisiertes Entfernen von Nutzungsbeschränkungen. Bei Apple-Geräten spricht man von Jailbreaking, bei Geräten mit Android von Rooting. Nach einem Jailbreak resp. Rooting kann das Gerät zum Beispiel Apps aus nicht autorisierten Quellen installieren.

Sicherheitssoftware und Sicherheitseinstellungen Ihres Gerätes einfach manipulieren oder Schadsoftware installieren. Arbeiten Sie deshalb immer mit minimalen Nutzerrechten. Gewähren Sie einer App nur die Berechtigungen, die sie zur Erfüllung ihrer Aufgabe zwingend benötigt. Verlangt zum Beispiel eine Taschenlampen-App Zugriff auf Ihre Kontakte, sollten Sie dies kritisch hinterfragen und sich ggf. nach Alternativen zu dieser App umsehen. Stellen Sie sicher, dass Ihr Antivirenprogramm regelmäßig (zum Beispiel ein Mal in der Woche) einen kompletten Suchlauf über alle Apps, Ordner und Dateien Ihres Gerätes durchführt.

Informationsquellen

Informieren Sie sich regelmäßig über Sicherheitsaspekte bei der Nutzung des Internets sowie geeignete Schutzmaßnahmen. Informationen dazu finden Sie auf der Internetseite Ihrer Bank, des Bankenverbandes (bankenverband.de), der Polizei (www.polizei-beratung.de) oder des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de und www.botfrei.de). Dort finden Sie auch kostenfreie Sicherheitssoftware.



3

Starten des Online-Bankings

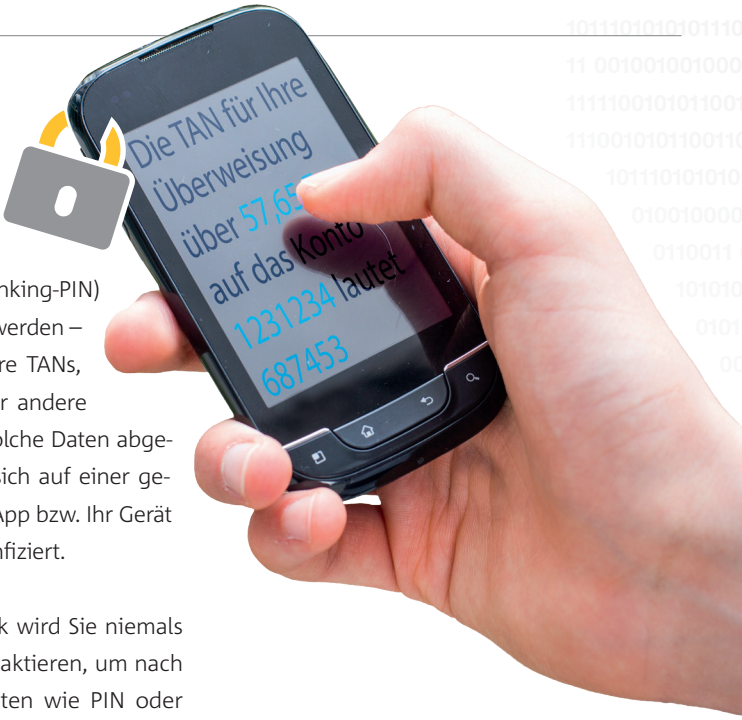
Um Ihre Online-Banking-Sitzung zu beginnen, rufen Sie in Ihrem Browser die Anmeldeseite Ihrer Bank auf. Auf keinen Fall sollten Sie unbesehen und unkontrolliert Web-Links aus Ihnen unbekannten Quellen verwenden, die Ihnen beispielsweise per E-Mail zugesandt wurden. Die drohende Gefahr hinter diesen Internetadressen: Es wird Ihnen eine täuschend echte, aber gefälschte Internetseite Ihrer Bank präsentiert, um Ihre geheimen Online-Banking-Zugangs-, Telefon-, Bankkarten- und andere persönliche Daten (Geburtstag, Adresse, Mädchenname usw.) auszuspähen und damit Missbrauch zu treiben.

Sehen Sie sich nun zunächst die Internetseite Ihrer Bank genau an. Sieht sie vertraut aus? Seien Sie wachsam! Sollten Sie eine Veränderung feststellen, zögern Sie nicht, bei Ihrer Bank telefonisch oder per E-Mail nachzufragen, ob das Layout der Seite verändert wurde.

Die Internetadresse zu Ihrem Online-Banking sollte mit „https“ beginnen. Das „https“ steht für eine sogenannte SSL/TLS-Verbindung, die für die Dauer Ihrer Online-Banking-Sitzung für eine verschlüsselte und damit gesicherte Übertragung zwischen Ihrem Browser und dem Bankrechner sorgt. Das Gleiche gilt für das Schlüssel- oder Schlosssymbol in Ihrem Browser. Es muss entweder das Schlosssymbol oder „https“ angezeigt werden und während der gesamten Online-Banking-Sitzung zu sehen sein. Sollte beides fehlen, melden Sie dies umgehend Ihrer Bank.

Bevor Sie zum ersten Mal Mobile-Banking nutzen, sollten Sie eine geeignete App für den Zugang zu Ihrer Bank aus dem autorisierten App-Store Ihres Smartphones oder Tablets beziehen und installieren. Hierfür sollten Sie keinen „Hinweisen“ aus E-Mails oder Webseiten nachgehen. Starten Sie nun Ihre Banking-App. Sieht sie vertraut aus?

3



Bei der Anmeldung zu Ihrem Konto dürfen nur die üblichen Online- bzw. Mobile-Banking-Zugangsdaten (Kundenkennung und Online-Banking-PIN) abgefragt und eingegeben werden – keinesfalls eine oder mehrere TANs, die Telefon-Banking-PIN oder andere persönliche Daten. Sollten solche Daten abgefragt werden, befinden Sie sich auf einer gefälschten Internetseite oder App bzw. Ihr Gerät ist mit einer Schadsoftware infiziert.

Wichtig zu wissen: Ihre Bank wird Sie niemals per E-Mail oder Telefon kontaktieren, um nach Ihren geheimen Zugangsdaten wie PIN oder TAN zu fragen oder um mit Ihnen gemeinsam eine Transaktion zur Verifizierung von Daten durchzuführen. Folgen Sie keinen Anweisungen, auch nicht unter Androhung negativer Konsequenzen wie beispielsweise einer Kontosperre. Informieren Sie umgehend Ihre Bank über jeden Betrugsversuch!

Schützen Sie Ihre PIN und Ihre Transaktionsnummern (kurz TANs) sowie die abhängig vom Sicherheitsverfahren Ihrer Bank erforderlichen Geräte vor unberechtigtem Zugriff. Diese sind beispielsweise ein Mobiltelefon zum Empfang einer mobileTAN, ein Lesegerät für das photoTAN-Verfahren, ein TAN-Generator oder ein Lesegerät für das chipTAN-Verfahren inklusive Ihrer girocard. Verwenden Sie für die Anmeldung zum Online- und Mobile-Banking die Online-Banking-PIN bzw. ein sicheres Passwort, das Sie ausschließlich für Ihr Banking verwenden, geheim halten und in regelmäßigen Abständen ändern. Geben Sie es niemals weiter oder speichern Sie dieses nicht unverschlüsselt auf dem PC oder Smartphone. Geben Sie niemals Ihre geheimen Zugangsdaten (PIN/TAN) im Internet weiter.

In den Online-/Mobile-Banking-Bedingungen Ihrer Bank sind Ihre vertraglichen Sorgfaltspflichten zur Nutzung des Bankings und zur Geheimhaltung von PIN und TANs ausführlich geregelt. Diese Pflichten dienen dem Schutz des Online- und Mobile-Banking-Verfahrens im Interesse von Kunde und Bank.

4

Überprüfen des Kontostatus

Prüfen Sie im Online-Banking den Zeitpunkt der letzten Anmeldung. Sollten Sie zu dem Zeitpunkt nicht angemeldet gewesen sein, könnte ein Ihnen Unbekannter auf Ihr Konto zugegriffen haben. Informieren Sie in diesem Fall sofort Ihre Bank und ändern Sie Ihre Zugangsdaten. Merken oder notieren Sie sich immer den Zeitpunkt Ihrer letzten Online-Banking-Sitzung. Prüfen Sie regelmäßig und in kurzen Abständen Ihre Umsätze, Ihren Konto- und Depotstand. Wurden alle Überweisungen von Ihnen veranlasst? Auch die Überweisungen in den Vormerkungen? Andernfalls kontaktieren Sie umgehend Ihre Bank.

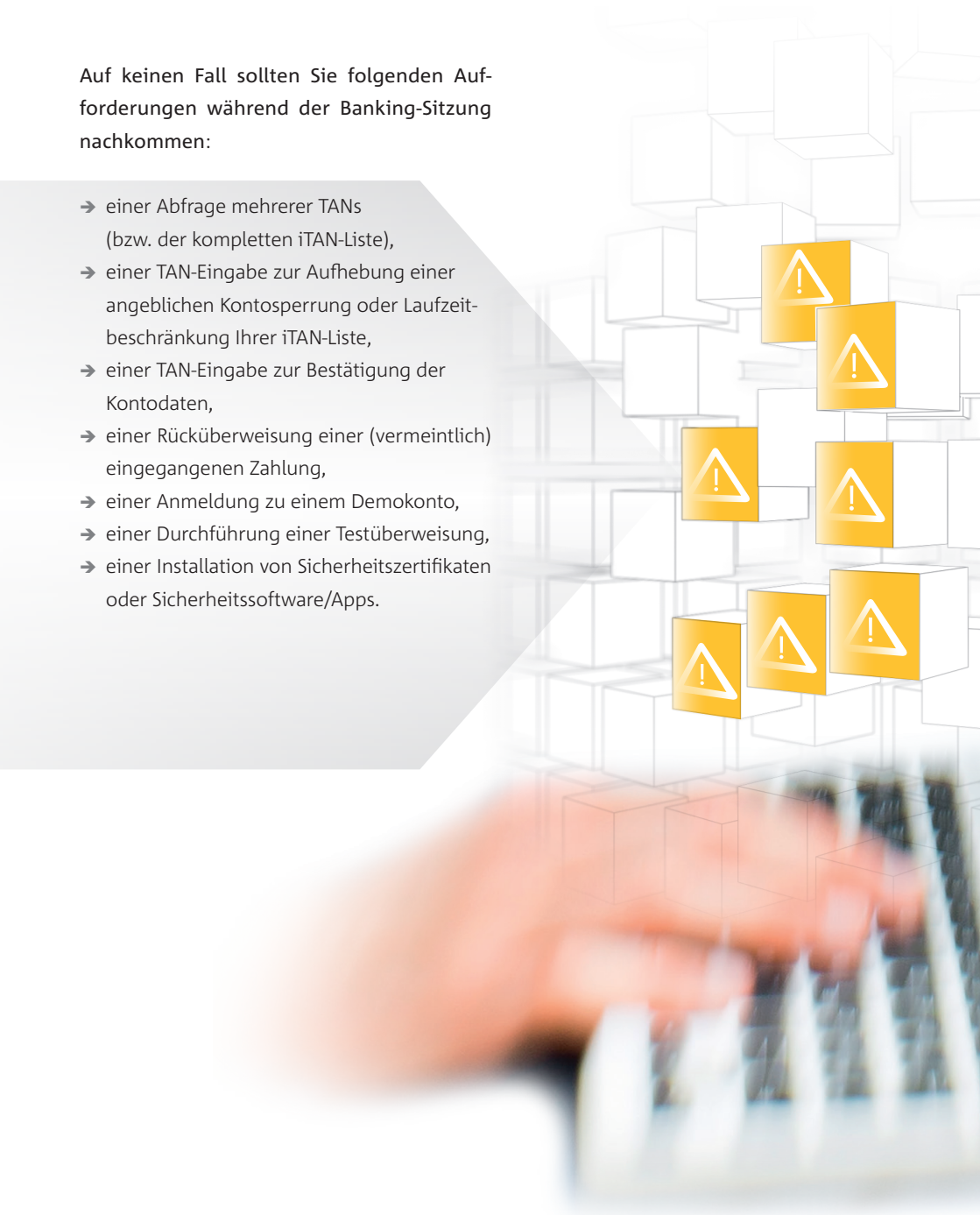
Sie sollten regelmäßig die Sicherheitseinstellungen Ihres Online- und Mobile-Bankings prüfen. Diese Einstellungen sind ebenfalls abhängig vom Angebot Ihrer Bank. So können Sie bei einigen Banken Überweisungslimits setzen oder ein Referenzkonto hinterlegen. Durch ein Limit können Sie festlegen, wie viel Geld maximal von Ihrem Konto einmalig oder in einem bestimmten Zeitraum überwiesen werden kann. Wenn Sie Geldfluss nur zu einem Referenzkonto erlauben, kann ein Dritter online Ihr Geld nicht ohne Weiteres auf ein anderes Konto überweisen. Ferner sollten Sie regelmäßig auch Ihre bei der Bank gespeicherten persönlichen Daten wie Postanschrift, E-Mail-Adresse oder Handynummer prüfen.

Warnung vor ungewöhnlichen TAN-Abfragen

Sie sollten immer die Sicherheitshinweise Ihrer Bank lesen. Vorsicht, wenn ein Sicherheitshinweis mit einer oder mehreren TANs quittiert werden soll – dies wird Ihre Bank niemals verlangen! Eine TAN wird generell nur nach Einstellung eines von Ihnen veranlassten konkreten Auftrags von Ihrer Bank abgefragt. Sollte zum Beispiel unmittelbar nach der Anmeldung zum Online-Banking die Bank eine TAN von Ihnen fordern, handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch. Dies geschieht meistens unter dem Vorwand, Sie hätten sich bei Ihrer letzten Online-Banking-Sitzung nicht korrekt abgemeldet oder es soll ein neues Sicherheitsverfahren getestet werden. Auch bei einer von Ihnen gewünschten Änderung Ihrer persönlichen Online-Banking-Einstellungen wird die Bank nur nach einer einzigen TAN – niemals nach mehreren TANs – fragen. Sollten Sie nach einer TAN auf eine Weise gefragt werden, die Ihnen ungewöhnlich vorkommt, brechen Sie den Vorgang sofort ab und kontaktieren Sie umgehend Ihre Bank per Telefon oder E-Mail.

Auf keinen Fall sollten Sie folgenden Aufforderungen während der Banking-Sitzung nachkommen:

- einer Abfrage mehrerer TANs (bzw. der kompletten iTAN-Liste),
- einer TAN-Eingabe zur Aufhebung einer angeblichen Kontosperrung oder Laufzeitbeschränkung Ihrer iTAN-Liste,
- einer TAN-Eingabe zur Bestätigung der Kontodaten,
- einer Rücküberweisung einer (vermeintlich) eingegangenen Zahlung,
- einer Anmeldung zu einem Demokonto,
- einer Durchführung einer Testüberweisung,
- einer Installation von Sicherheitszertifikaten oder Sicherheitssoftware/Apps.



5

Vornehmen einer SEPA-Überweisung

Füllen Sie wie gewohnt das SEPA[2)]-Überweisungsformular aus. Haben Sie bereits früher Überweisungsvorlagen angelegt, so verwenden Sie diese, natürlich erst nach Prüfung, ob alles richtig übernommen wurde. Denn ein Angreifer, der Zugriff auf Ihr Konto hatte, könnte auch diese Vorlagen manipuliert haben, indem er zum Beispiel die IBAN für Ihre monatliche Mietzahlung verändert hat. Sind die Überweisungsdaten korrekt, schicken Sie den Auftrag an Ihre Bank. Diese fordert Sie nun zur Eingabe einer – nicht zwei oder mehrerer – TAN auf. Bevor Sie diese eintippen und die Transaktion somit bestätigen, überprüfen Sie noch einmal die Überweisungsdaten. Benutzen Sie ein TAN-Verfahren mit einem Zusatzgerät wie zum Beispiel Handy/Smartphone beim mobileTAN-Verfahren, photoTAN-Gerät, chipTAN-Lesegerät, vergleichen Sie sorgfältig die Überweisungsdaten auf dem Display Ihres Gerätes mit den von Ihnen eingegebenen Überweisungsdaten. Beim mobileTAN-Verfahren wird die TAN per SMS auf Ihr Handy/Smartphone gesendet.

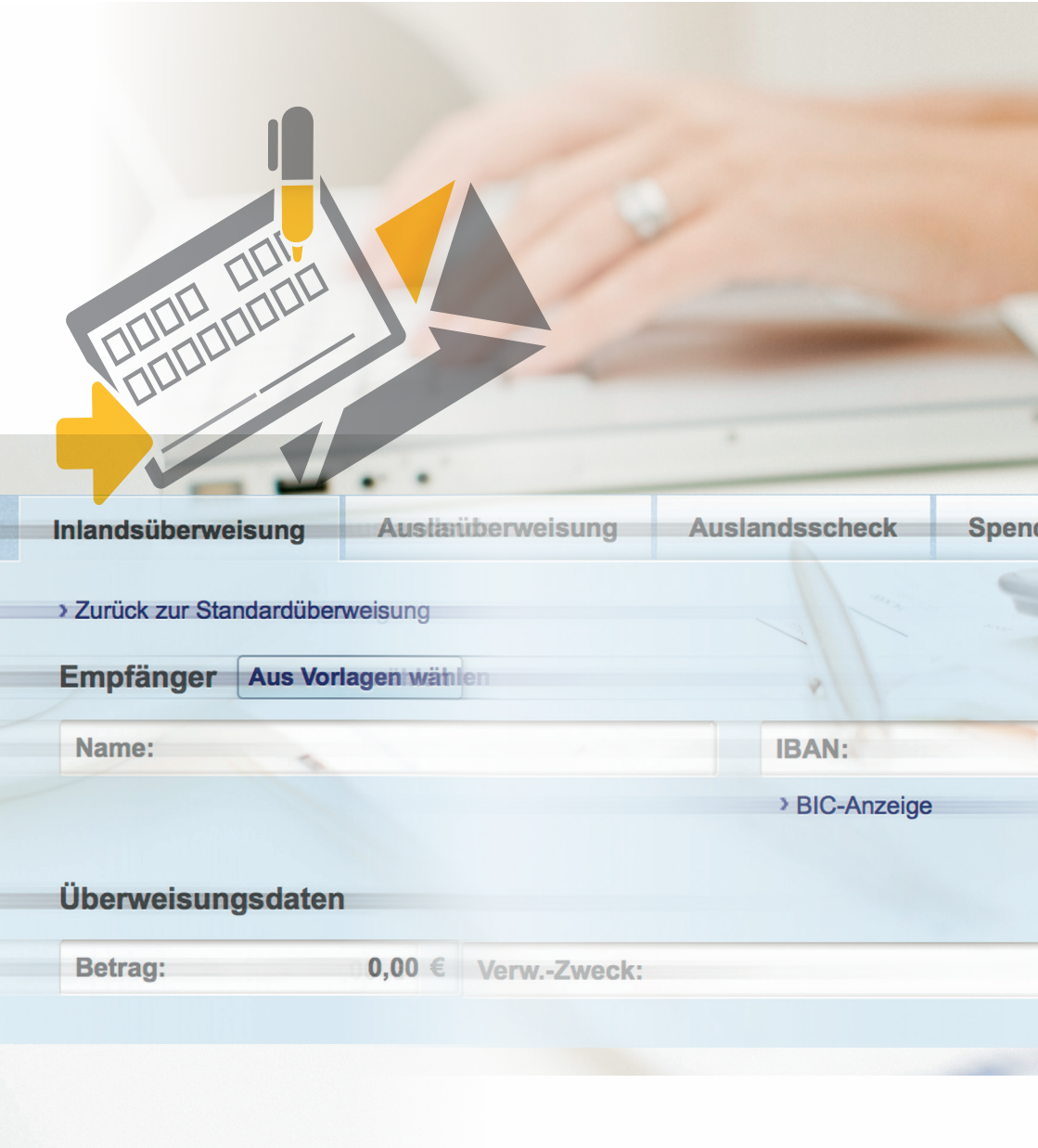
Sie können die Überweisung nun durch Bestätigung freigeben. Wird „TAN ungültig“ angezeigt, überprüfen Sie Ihre eingegebene TAN auf Tippfehler. Prüfen Sie nach Abschluss der Überweisung noch die Auftragsbestätigung. Bei einigen Banken erhalten Sie zusätzlich noch eine Bestätigungsnummer.

Nach Abschluss der Überweisung sollten Sie den aktuellen Kontostand überprüfen: Stimmen Umsatzübersicht und Kontostand? Sehen Sie sich die zuletzt vorgenommene Überweisung an. Stimmen Details wie Empfänger, Betrag, Verwendungszweck, Empfänger-IBAN und Empfängerbank?

Beenden Sie die Banking-Sitzung korrekt, indem Sie auf „Logout“ oder „Abmelden“ in der Banking-Anwendung klicken. Sie sollten nicht einfach den Internetbrowser oder die App schließen, ohne sich vorher ordnungsgemäß abzumelden. Merken Sie sich, wann Sie das letzte Mal die „persönliche Bankfiliale“ per Online- oder Mobile-Banking besucht haben.

Zu guter Letzt: Überprüfen Sie regelmäßig Ihren beleghaften beziehungsweise elektronischen Kontoauszug sowie Ihre Konto-, Wertpapier- und Kreditkartenumsätze.

2) SEPA ist die Abkürzung für Single Euro Payments Area und bezeichnet den einheitlichen europaweiten Zahlungsraum für Transaktionen in Euro.


Inlandsüberweisung
Auslandsscheck
› Zurück zur Standardüberweisung
Empfänger
Aus Vorlagen wählen
Name:
IBAN:
› BIC-Anzeige
Überweisungsdaten
Betrag:
0,00 €
Verw.-Zweck:

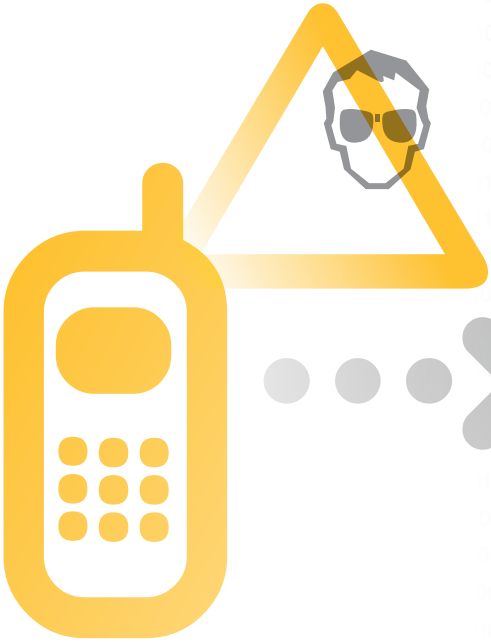
6

Bei Verdacht

Stellen Sie fest, dass die Online-Banking-Seite oder die App Ihrer Bank gefälscht ist oder ist erkennbar, dass ein Dritter Zugriff auf Ihr Konto hatte oder haben könnte, so kontaktieren Sie umgehend Ihre Bank: Rufen Sie die Hotline an! Alternativ können Sie eine E-Mail schicken – am besten mit einer Bildschirmkopie (engl. Screenshot). Führen Sie auf keinen Fall weiter Banking-Transaktionen aus, sondern besprechen Sie die weitere Vorgehensweise mit Ihrer Bank. Lassen Sie umgehend den Online-/Mobile-Banking-Zugang zu Ihrem Konto vorsorglich sperren.

Ist erkennbar, dass von Ihrem Konto bereits Geld abgeflossen ist oder andere unautorisierte Transaktionen vorgenommen wurden, informieren Sie sofort Ihre Bank und erstatten Sie Anzeige bei der Polizei. Zur weiteren Schadensabwehr sollten Sie auch Ihre Kreditkartenumsätze prüfen. Zudem sollten Sie die Zugangsdaten zu all Ihren genutzten Online-Diensten wie zum Beispiel E-Mail-Konten, Onlineshops und soziale Netzwerke vorsichtshalber sperren. Darüber hinaus sollten Sie alle Personen warnen, die Ihr Gerät mitbenutzen – denn vielleicht hat der Angreifer auch versucht, deren persönliche Zugangsdaten auszuspionieren.

Der beste Weg zu einem sauberen PC ist die Neuinstallation durch einen Fachmann. Danach aktualisieren Sie Betriebssystem, Anwendungssoftware und Sicherheitssoftware (zum Beispiel Antivirenprogramm und Personal Firewall). Eine Aktualisierung ohne Neuinstallation ist gegebenenfalls nicht ausreichend. Ändern Sie erst jetzt alle Ihre Zugangsdaten.



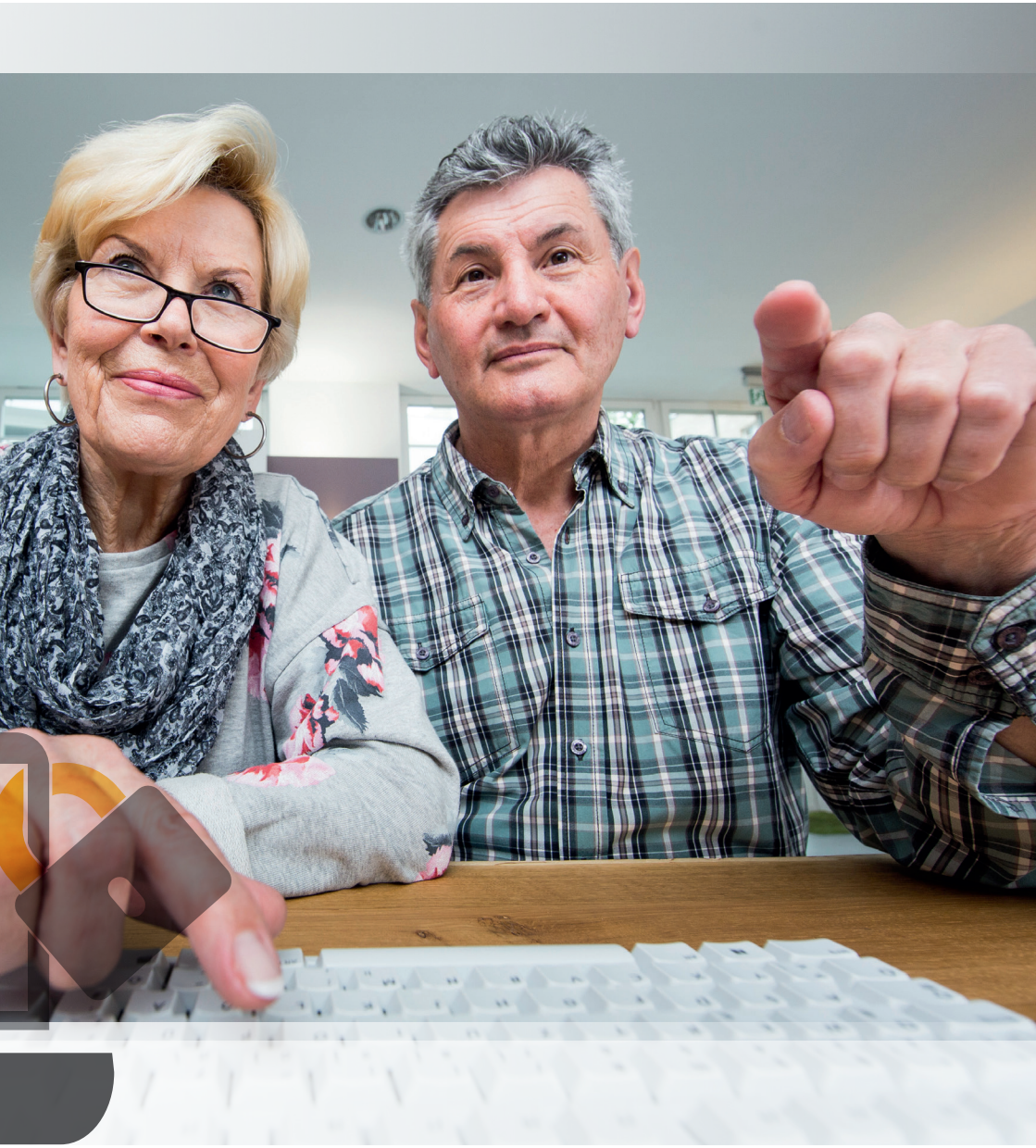
7

Ja zum Online-Banking – aber nicht im Namen Dritter

Auf Internetseiten und per E-Mail sprechen Kriminelle immer wieder Inhaber von Bankkonten an, um sie für eine Tätigkeit als sogenannter „Finanzagent“, „Warenagent“ oder auch „Kontovermieter“ zu gewinnen. Stellen Sie Ihr Bankkonto Dritten – bewusst oder unbewusst – nicht für betrügerische Finanztransaktionen zur Verfügung. Sie machen sich strafbar! Über diese Betrugsarten informiert Sie ausführlich das Faltblatt „Dubioses Stellenangebot: Finanzagent“ des Bankenverbandes.

Die wichtigsten Sicherheitshinweise im Überblick

- Verwenden Sie Ihren gesunden Menschenverstand.
- Halten Sie Ihre Online- und Mobile-Banking-Geräte aktuell – Software und Hardware.
- Aktivieren Sie die automatische Update-Funktion.
- Installieren Sie Softwareupdates, sobald diese verfügbar sind.
- Setzen Sie Sicherheitssoftware (mindestens Antivirenprogramm und Personal Firewall) ein.
- Verwenden Sie immer die aktuellste Version Ihres Internetbrowsers/Ihrer Banking-App.
- Öffnen Sie keine E-Mails, SMS und Anhänge von unbekannten Absendern.



Online- und Mobile-Banking –

bequem und sicher über Browser und App

- Kontrollieren Sie immer Ihren Auftrag vor Freigabe auf Korrektheit.
- Geben Sie immer nur eine einzige TAN zur Freigabe ein.
- Prüfen Sie regelmäßig Ihre Kontoauszüge.
- Halten Sie Software und Apps Ihrer Online- und Mobile-Banking-Geräte aktuell.

Die Reihe „fokus | verbraucher“

Informationen, die sich gezielt an Verbraucher wenden, fasst der Bankenverband in einer eigenen Reihe „fokus | verbraucher – eine Information der privaten Banken“ zusammen. Hier erhalten Verbraucher kostenfrei fundierte Informationen in leicht verständlicher Form. Folgende Publikationen sind in der Reihe zuletzt erschienen:

SEPA ist da – einfach bezahlen mit IBAN und BIC
Berlin, Januar 2016, Faltblatt

Bargeldlos bezahlen
Berlin, August 2015, Broschüre

Pfändungsschutz dank P-Konto
Berlin, Juli 2015, Faltblatt

Sicher mit Karte
Sicherheitstipps zur Bankkarte
Berlin, Juni 2015, Faltblatt

Der Ombudsmann der privaten Banken – Fragen und Antworten
Berlin, Mai 2015, Faltblatt

Frühzeitig für Notfälle Bankangelegenheiten regeln
Berlin, April 2015, Faltblatt

Vorsicht: Betrug per Telefon
Berlin, März 2015, Faltblatt

Änderungen beim Einlagensicherungsfonds
Berlin, Oktober 2014, Faltblatt

Wie schütze ich mich vor Phishing?
Berlin, August 2014, Faltblatt

Dubioses Stellenangebot: Finanzagent
Berlin, Juli 2014, Faltblatt

Tipps für die Anlageberatung
Berlin, September 2013, Faltblatt

Alle Publikationen können unter **www.bankenverband.de** kostenfrei bestellt werden oder als PDF-Datei heruntergeladen werden. Stand: Oktober 2016.

Impressum

Herausgeber	Bundesverband deutscher Banken e. V. Postfach 040307, 10062 Berlin
Verantwortlich	Iris Bethge
Druck	PieReg Druckcenter Berlin
Gestaltung	doppel:punkt redaktionsbüro janet eicher, Bonn
Fotos	action press, Jochen Zick
Gedruckt	November 2016

So erreichen Sie den Bankenverband

Per Post:
Bundesverband deutscher Banken
Postfach 040307
10062 Berlin

Per Telefon:
+49 30 1663-0

Per Fax:
+49 30 1663-1399

Per E-Mail:
bankenverband@bdb.de

Im Internet:
bankenverband.de

Scannen Sie diesen QR-Code, um weiterführende Informationen zu erhalten.

Social Media:

twitter.com/bankenverband

youtube.com/user/bankenverb

flickr.com/photos/bankenverband