

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Christian Görke, Janine Wissler, Doris Achelwilm, weiterer Abgeordneter und der Fraktion Die Linke
– Drucksache 21/1825 –**

Betrugsfälle beim Online-Banking in Deutschland

Vorbemerkung der Fragesteller

Durch immer professionellere Methoden werden private Bankkunden immer häufiger Opfer von Online-Betrug. Die Schäden gehen mindestens in zweistellige Milliardenhöhen (www.test.de/Online-Banking-Wie-Sie-Betrueger-aus-bremsen-6149442-0).

Betroffen sind hiervon auch zahlreiche Kunden der Postbank (siehe www.anwalt.de/rechtstipps/vermehrte-betrugsfaelle-bei-postbank-und-co-240522.html). Laut Geschädigten, die sich an die Fragestellenden gewendet haben, bleiben diese unter anderem auf ihren Verlusten sitzen, weil die Postbank argumentiert, die Betroffenen hätten „grob fahrlässig“ gehandelt.

Laut Postbank handelt es sich bei dem von ihr zur Authentifizierung verwendeten BestSign-Verfahren um ein „nicht manipulierbares kryptographisches Verfahren“ (siehe www.anwalt.de/rechtstipps/zahlreiche-postbank-kunden-beklagen-kontopluenderung-nach-aktivierung-des-bestsign-verfahrens-251840.html). Dies muss aus Sicht der Fragestellenden angesichts der zunehmenden Betrugsfälle infrage gestellt werden. Anwälte verweisen darauf, dass das BestSign-Verfahren Schwächen hat (siehe www.prigge-recht.de/postbank-konto-gehackt-was-tun und www.youtube.com/watch?v=NBn8pZELdWY).

Bei der Postbank lässt sich der Verfügungsrahmen für Online-Überweisungen sofort ändern, wodurch unmittelbar danach größere Summen vom betroffenen Konto abgebogen werden können, während zum Beispiel bei der Muttergesellschaft Deutsche Bank eine Änderung erst mit Verzögerung aktiv wird (www.abendblatt.de/hamburg/wirtschaft/article409469620/haspa-postbank-ing-ueberweisungen-werden-ploetzlich-abgelehnt.html).

Zu Problemen bei der Postbank kam es offensichtlich speziell seit der Integration in die Systeme der Deutschen Bank (www.tagesschau.de/wirtschaft/finanzen/bafin-deutsche-bank-probleme-post-bank-100.html). 2023 bestellte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) deshalb einen Sonderbeauftragten (www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2023/meldung_2023_09_04_Postbank.html).

1. Wie viele Fälle von Online-Banking-Betrug hat es nach Kenntnis der Bundesregierung im Jahr 2024 in Deutschland gegeben, und wie viele davon ereigneten sich bei der Postbank bzw. wie viele davon bei anderen Banken?
2. Teilt die Bundesregierung den Eindruck der Fragestellenden, dass sich die Zahl der Online-Banking-Betrugsfälle in den vergangenen Jahren signifikant erhöht hat (bitte Antwort begründen und, wenn möglich, mit Zahlen aus den letzten fünf Jahren belegen)?

Die Fragen 1 und 2 werden gemeinsam beantwortet.

Die offiziellen, europaweit einheitlichen Statistiken im Bereich Zahlungsbetrug werden von der Europäischen Bankenaufsichtsbehörde (EBA) und der Europäischen Zentralbank (EZB) veröffentlicht. Der aktuelle Bericht („Report on payment fraud 2024“) stammt aus dem August 2024 und bezieht sich auf den Zeitraum des Jahres 2022 sowie des ersten Halbjahres 2023. Über diese Datenquelle hinaus liegen der Bundesregierung keine gesicherten und umfassenden Statistiken im Bereich Zahlungsbetrug vor.

„Online-Banking-Betrugsfälle“ sind keine Kategorie dieser offiziellen Statistiken, sodass die Fragen 1 und 2 nicht konkret beantwortet werden können.

3. Wie viele Betrugsfälle bei der Postbank wurden nach Kenntnis der Bundesregierung im Jahr 2024 bei der Polizei zur Anzeige gebracht?
4. Bei wie vielen der in der Frage 3 genannten Fälle wurden die Ermittlungen erfolgreich abgeschlossen, bei wie vielen erfolgte eine Einstellung des Verfahrens, und bei wie vielen dauern die Ermittlungen noch an?

Die Fragen 3 und 4 werden gemeinsam beantwortet.

Auf die Antwort zu den Fragen 1 und 2 wird verwiesen. Die Statistiken im Bereich Zahlungsbetrug werden von EBA und EZB in aggregierter Form veröffentlicht, sodass keine Aussagen über einzelne Institute getroffen werden können.

5. Inwieweit erfolgt in diesem Bereich der Finanzkriminalität mit Online-Banking-Betrugsfällen eine länderübergreifende Zusammenarbeit der Polizeibehörden unter Mitwirkung des Bundeskriminalamts (BKA), der Bundesanstalt für Finanzdienstleistungsaufsicht, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und weiterer Bundesbehörden?

Die Erfassung und Bearbeitung von Online-Banking-Betrugsfällen mit dem Modus Operandi Phishing, auf die sich die Anfrage bezieht, liegen in der Zuständigkeit der Strafverfolgungsbehörden der Länder. Das Bundeskriminalamt (BKA) unterstützt die Landesbehörden im Rahmen seines gesetzlichen Auftrages als Zentralstelle der deutschen Polizei, zum Beispiel bei der Durchführung vom nationalen und internationalen Schriftverkehr bei Straftaten mit länder- oder grenzübergreifender Bedeutung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird über IT-Sicherheitsvorfälle bei größeren Finanzinstituten („kritische Infrastrukturen“) informiert. Es erfolgt in der Regel keine direkte Information durch betroffene Bürgerinnen und Bürger an das BSI bzw. keine Information, wenn Einzelpersonen betroffen sind. Erste Anlaufstellen sind hier die zuständigen Polizeibehörden sowie die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Das BSI steht mit der BaFin in Kontakt.

Die BaFin wird im Rahmen ihrer Aufgaben und abhängig vom Einzelfall als Aufsichtsbehörde in der Regel von den Strafverfolgungsbehörden über einzelne Strafverfahren mit Bezug zu Finanzkriminalität informiert, soweit Objekte unter ihrer Aufsicht Gegenstand des Verfahrens sind oder wenn diese die Anforderungen aus Aufsichtsgesetzen, wie zum Beispiel dem Kreditwesengesetz oder dem Geldwäschegesetz (GwG) nicht einhalten.

Die Zentralstelle für Finanztransaktionsuntersuchungen wertet Meldungen über verdächtige Finanztransaktionen, die unter anderem im Zusammenhang mit Geldwäsche und damit zusammenhängenden Vortaten stehen könnten, aus, reicht sie an und übermittelt bei Vorliegen der zugehörigen Voraussetzungen das Ergebnis ihrer Analyse gemäß § 32 Absatz 2 Satz 1 GwG an die zuständigen Strafverfolgungsbehörden. Hierbei besteht nach Maßgabe von § 30 Absatz 2 Satz 6, 7 GwG ein laufender Beteiligungsprozess insbesondere mit den Strafverfolgungsbehörden des Bundes und der Länder.

Der Deliktbereich des Betruges als geldwäschebezogene Vortat stellt einen vereinbarten Risikoschwerpunkt bei der Analyse der Financial Intelligence Unit (FIU) dar. Bei der Ausgestaltung der Prozesse wird den BSI-Standards laufend entsprochen.

6. In wie vielen Fällen haben nach Kenntnis der Bundesregierung Kunden der Postbank, die im Jahr 2024 (oder ggf. im letzten Jahr, für das Daten vorliegen) Opfer eines Betruges wurden, eine Rückerstattung des Geldes von der Postbank gefordert?
7. In wie vielen der in der Frage 6 genannten Fälle
 - a) hat die Postbank den zu Unrecht abgebuchten Betrag zurückerstattet,
 - b) erfolgte eine Teilerstattung (aus Kulanz, infolge eines Vergleichs bzw. einer Güteverhandlung),
 - c) erfolgte keine Erstattung mit dem Verweis der Postbank, dass der Kunde bzw. die Kundin „grob fahrlässig“ gehandelt habe,
 - d) entschied ein Gericht zugunsten der Postbank bzw.
 - e) entschied ein Gericht, dass die Postbank den Betrag zu erstatten hat, weil das Betrugsopfer nicht „grob fahrlässig“ gehandelt habe (oder aus anderen Gründen)?

Die Fragen 6 und 7 werden gemeinsam beantwortet.

Die Vertragsbeziehung zwischen einem Kreditinstitut und seinen Kunden ist grundsätzlich privatrechtlicher Natur. Der Bundesregierung liegen daher keine gesammelten Informationen zur Beantwortung dieser Fragen vor.

8. Welche Haltung hat die Bundesregierung grundsätzlich zu der Frage, was unter „grober Fahrlässigkeit“ im Zusammenhang mit Online-Banking-Betrug zu verstehen ist (bitte konkret ausführen, welches Verhalten darunterfällt und welches nicht)?

Bei einer unautorisierten Zahlung steht dem Zahlungsdienstnutzer grundsätzlich ein Rückerstattungsanspruch gegen seinen Zahlungsdienstleister nach § 675u Satz 2 des Bürgerlichen Gesetzbuches (BGB) zu. Dieser Rückerstattungsanspruch kann im Einzelfall ausgeschlossen sein, wenn der Zahlungsdienstnutzer die unautorisierte Zahlung durch eigenes grob fahrlässiges Verhalten (mit-)verursacht hat. Eine grobe Fahrlässigkeit liegt bei Missachtung der erforderlichen Sorgfalt in besonders schwerem, ungewöhnlich hohem Maße,

bei der selbst ganz naheliegende Überlegungen nicht angestellt und dasjenige unbeachtet gelassen wird, was jedem einleuchten müsste, vor.

Die Entscheidung, ob im Einzelfall ein grob fahrlässiges Verhalten vorliegt, erfolgt unter Berücksichtigung aller Umstände des Einzelfalls und obliegt der Rechtsprechung. Im Rahmen der Einzelfallbetrachtung werden auch die steti-ger Weiterentwicklung unterliegenden technischen Möglichkeiten berücksichtigt.

9. Welche Maßnahmen haben das zuständige Bundesministerium, das BKA, die BaFin, das BSI und weitere Bundesbehörden ergriffen, um gegen den Online-Banking-Betrug erfolgreicher vorzugehen und die privaten Bankkunden besser zu schützen (bitte einzeln mit Zeitpunkt auflisten und beschreiben)?

Zur Sensibilisierung von Bürgerinnen und Bürgern gegenüber Phishing-Betrugsstraftaten wurden auf der BKA-Homepage ein Warnhinweis zu Phishing/Identitätsdiebstahl sowie Empfehlungen zum Schutz vor solchen Vorfällen veröffentlicht: BKA – Identitätsdiebstahl/Phishing. Die Homepage enthält zudem Verlinkungen zu weiteren Websites, zum Beispiel zu der des BSI mit ausführlicheren Informationen zur digitalen Sicherheit.

Im Rahmen der Wahrnehmung seiner Zentralstellenfunktion werden vom BKA Informationen zu Betrugsfällen aus dem Bundesgebiet gesammelt und analysiert. Sollten überregionale oder internationale Zusammenhänge festgestellt werden, können zentrale Ermittlungen initiiert werden. Zurzeit werden zentrale Ermittlungen von einer Landespolizeidienststelle im Zusammenhang mit Phishing-as-a-Service (Angebot krimineller Dienstleistungen und Tools) geführt, das BKA nimmt im Verfahren eine koordinierende Funktion wahr.

Das BSI informiert fortlaufend über verschiedene Kanäle zum Thema Sicherheit beim Online-Banking:

- Informationen an Verbraucherinnen und Verbraucher: Internetseiten „Onlinebanking, Onlineshopping und mobil bezahlen“ unter www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/online-banking-online-shopping-und-mobil-bezahlen_node.html sowie die sich darunter befindende Seite zu zum Thema „Online-Banking“
- Informationen an Verbraucherinnen und Verbraucher: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen-und-Buerger/buergerinnen-und-buerger_node.html
- Informationen zur allgemeinen IT-Sicherheit im BSI-Newsletter „Einfach – Cybersicher“

Allgemein sensibilisiert das BSI zu Themen wie „E-Mail-Sicherheit“ oder „Phishing“, welche ein häufiges Einfallstor für Angriffe auf das Online-Banking sind, auf seinen Internetseiten und über die Social-Media-Kanäle.

Zudem informiert die BaFin – sowohl auf der Website als auch in gedruckter Form – unter anderem über gängige Betrugsmaschen in Zusammenhang mit Online-Banking-Betrug. Die BaFin gibt Hilfestellungen dazu, wie sich Verbraucherinnen und Verbraucher vor betrügerischen Verhaltensweisen schützen können. Im Einzelnen:

- Finanzen.Information.Tipps Ausgabe 1/2024: www.bafin.de/ref/19706126 und Ausgabe 05/24 (www.bafin.de/ref/19735808): In den Formaten „Digitale Finanzgeschäfte – neue Wege, sichere Möglichkeiten“ und „Sicher am

Finanzmarkt – Betrugsmaschinen“ wird unter anderem Phishing (im Deutschen: Passwort fischen) als häufige Betrugsmaschine vorgestellt.

- Verbraucherinformation auf der Website „Phishing & Co.: Vorsicht im Umgang mit sensiblen Daten!“, www.bafin.de/ref/19642304

Die Financial Intelligence Unit (FIU) veröffentlicht zum Schutz privater Bankkunden im Rahmen ihrer Zuständigkeit anlassbezogen Warnhinweise auf ihrer Webseite:

Warnung vor betrügerischen (Phishing-)E-Mails im Namen der FIU Deutschland, womit die Betroffenen aufgefordert werden, personenbezogene Daten mitzuteilen und Überweisungen zu tätigen; eingestellt am 18. September 2025 (www.zoll.de/DE/FIU/Aktuelles-FIU-Meldungen/2025/fiu_warnung_betrug_email_1.html?nn=126524).

In Bezug auf die Zahlungsdienstleister bestehen seit der Umsetzung sicherheitstechnischer Anforderungen der Richtlinie (EU) 2015/2366 (Payment Services Directive 2, kurz PSD 2) zum 14. September 2019 aufsichtsrechtliche Pflichten der Zahlungsdienstleister, die Betrugsfälle im Zahlungsverkehr bekämpfen sollen (insbesondere Starke Kundenauthentifizierung und Transaktionsüberwachung). Die BaFin beaufsichtigt die Zahlungsdienstleister hinsichtlich der Einhaltung dieser aufsichtlichen Anforderungen. Zu beachten ist, dass es sich bei der PSD 2 um eine europäische Vollharmonisierungsrichtlinie handelt, das heißt auf nationaler Ebene können weder strengere noch weniger strenge Anforderungen umgesetzt werden.

10. In welcher Höhe sind der Bundesregierung Schäden für Verbraucherinnen und Verbraucher bekannt, die auf Finanzkriminalität bei Zahlungsdienstleistern zurückzuführen sind?

Es wird auf die Antwort der Bundesregierung zu Frage 17 der Kleinen Anfrage „Verdacht auf Geldwäsche und Finanzkriminalität – Vorwürfe gegen Zahlungsdienstleister“ der Fraktion Die Linke auf Bundestagsdrucksache 21/1343 verwiesen.

11. Welche Voraussetzungen müssen nach Kenntnis der Bundesregierung Zahlungsdienstleister erfüllen, um Risiken im Zahlungsverkehrsbereich effektiv zu begrenzen?

Zahlungsdienstleister müssen die europarechtlich vorgegebenen Anforderungen der PSD 2 erfüllen. Diese europarechtlichen Anforderungen sind für das Vertragsverhältnis zwischen Zahlungsdienstleister und -nutzer in den §§ 675c folgend BGB umgesetzt. Diese Vorschriften sehen auch gewisse Pflichten für Zahlungsdienstleister bzw. Maßnahmen vor, um Zahlungsvorgänge sicher zu gestalten.

Gemäß § 675k Absatz 1 BGB können Zahlungsdienstleister und -nutzer Betragsobergrenzen für die Nutzung eines Zahlungsinstrumentes vereinbaren. Zudem können sie bestimmen, dass der Zahlungsdienstleister das Recht hat, ein Zahlungsinstrument unter bestimmten, die Sicherheit des Zahlungsinstrumentes beeinträchtigenden Umständen oder bei Verdacht einer betrügerischen Verwendung zu sperren; § 675k Absatz 2 Satz 1 BGB. Zudem treffen den Zahlungsdienstleister weitere, die Sicherheit von Zahlungen bzw. Zahlungsinstrumenten gewährleistende Pflichten in Bezug auf Zahlungsinstrumente gemäß § 675m BGB.

Im Rahmen der auf EU-Ebene geführten Verhandlungen zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010 (Payment Services Regulation, im Folgenden: PSR) und zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt, zur Änderung der Richtlinie 98/26/EG und zur Aufhebung der Richtlinien (EU) 2015/2366 und 2009/110/EG (Payment Services Directive 3, im Folgenden: PSD 3) werden zudem weitergehende Maßnahmen diskutiert, um Risiken im Zahlungsverkehr zu begrenzen.

Diese diskutierten Maßnahmen beinhalten einerseits eine Pflicht von Zahlungsdienstleistern zur Transaktionsüberwachung mit entsprechenden Blockierungsmöglichkeiten von Zahlungen für Zahlungsdienstleister, die Einrichtung von Ausgabenobergrenzen durch Zahlungsdienstnutzer, die Etablierung von sogenannten „Cooling-off-periods“, das heißt die Einrichtung einer gewissen Wartezeit, nach der erstmalig nach dem Erhöhen einer Ausgabenobergrenze Zahlungen vorgenommen werden können sowie andererseits Maßnahmen zum Austausch von Informationen zu betrügerischen Zahlungen zwischen Zahlungsdienstleistern. Nach Auffassung der Bundesregierung sind die vorgeschlagenen Regelungen geeignet, die Betrugsbekämpfung zu verbessern.

Darüber hinaus fallen Zahlungsdienstleister auch in den Anwendungsbereich des Digital Operational Resilience Act, welcher weitere Risiken auch außerhalb des Zahlungsverkehrs erfasst.

12. Inwieweit ist nach Kenntnis der Bundesregierung das von der Postbank verwendete BestSign-Verfahren sicher, und gibt es nach Kenntnis der Bundesbehörden Fälle, in denen das BestSign-Verfahren Schwächen zeigte (siehe Vorbemerkung der Fragestellenden)?

Der Bundesregierung liegen keine Erkenntnisse zum BestSign-Verfahren vor. Viele der derzeit zu beobachtenden typischen Betrugsversuche können unabhängig von der sicherheitstechnischen Ausgestaltung der Authentifizierungsverfahren erfolgreich sein. Zugangsdaten und Daten zur Autorisierung von Zahlungen werden durch Phishing beziehungsweise Social-Engineering-Angriffe abgegriffen. In manchen Fällen autorisieren die getäuschten Opfer die Zahlungen auch selbst.

13. Welche Abwicklungsverfahren für Zahlungen bei Zahlungsdienstleistern hält die Bundesregierung für sicher (bitte sowohl Merkmale beschreiben als auch einzelne benennen)?

Abwicklungsverfahren für Zahlungen bei Zahlungsdienstleistern müssen den aufsichtlichen Anforderungen der PSD 2 entsprechen, die die Sicherheit der Verfahren garantiert. Als Orientierung hat die EBA unter anderem eine „Opinion on the elements of Strong Customer Authentication“ (siehe EBA publishes an Opinion on the elements of strong customer authentication under PSD2 | European Banking Authority) veröffentlicht.

14. Inwieweit hält es die Bundesregierung für geboten, dass die Postbank und weitere Banken den Verbraucherschutz dadurch erhöhen, dass die Änderung des Verfügungsrahmens für Online-Überweisungen nicht mehr online unmittelbar vor einer Online-Überweisung erfolgen kann (siehe Vorbemerkung der Fragestellenden)?

Wie bereits in der Antwort zu Frage 11 aufgeführt wird auf europäischer Ebene im Rahmen der PSR/PSD 3-Verhandlungen derzeit über die Einführung einer sogenannten „Cooling-off-period“ diskutiert. Diese würde bewirken, dass nach Erhöhung eines Verfügungsrahmens nicht unmittelbar eine Zahlung vorgenommen werden kann, sondern dies erst nach Ablauf einer gewissen Zeitspanne möglich wäre. Die Bundesregierung unterstützt dies.

15. Wie ist der Stand der Arbeit des von der BaFin bestellten Sonderbeauftragten (www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2023/meldung_2023_09_04_Postbank.html), und welche Erkenntnisse gibt es insbesondere zu der Frage, was die Postbank an Maßnahmen ergriffen hat, um die Situation zu verbessern?
16. Wie viele Problemfälle mit welchem Finanzvolumen hat die BaFin im Rahmen der Tätigkeit des in der Frage 15 genannten Sonderbeauftragten identifiziert, und wie viele davon wurden inzwischen behoben bzw. entschädigt?

Die Fragen 15 und 16 werden gemeinsam beantwortet.

Das Mandat des Sonderbeauftragten beinhaltet die Überwachung der nachhaltigen und vollständigen Beseitigung der 2023 aufgetretenen vielschichtigen und umfangreichen Einschränkungen im Kundenservice. Sein Fokus ist darauf gerichtet, dass das Institut Maßnahmen ergreift, um Aufträge von Kundinnen und Kunden in einer angemessenen Frist zu bearbeiten und seinerzeit rückständige nicht bearbeitete Kundenaufträge rasch abzuarbeiten. Das Mandat des von der BaFin bestellten Sonderbeauftragten umfasst keine spezifischen Betrugsthemen, sodass die Frage 16 zu der Anzahl der Problemfälle und dem dazugehörigen Finanzvolumen nicht beantwortet werden kann.

