verbraucherzentrale
Bundesverband

BANK ODER BETRÜGER?

Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr

9. Mai 2024

Impressum

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Team Marktbeobachtung Finanzmarkt
MBFinanzmarkt@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.

INHALT

VERBRAUCHERRELEVANZ

Betrug im Zahlungsverkehr nimmt seit Jahren zu. Die Konten von Verbraucher:innen stehen immer mehr im Fokus von Betrüger:innen: Phishing-Mails, Anrufe von angeblichen Bankmitarbeiter:innen, Nachrichten per SMS und über Messenger-Dienste – sie alle haben das eine Ziel: Das Geld der Verbraucher:innen.

Im vergangenen Jahr wurden die Schadenssummen durch derartigen Betrug immer höher und die Aufklärungsquote sank. Bei den Verbraucherzentralen stiegen die Beschwerden über Cyberkriminalität im Zusammenhang mit Finanzdienstleistungen erheblich an. Denn: Trotz einer auf den ersten Blick verbraucherfreundlichen Regelung zur Haftung in derartigen Betrugsfällen scheint die Abwicklung in der Praxis wiederholt nicht gut zu funktionieren. Verbraucher:innen bleiben immer wieder auf den teils hohen Schäden sitzen. Ihre Banken und Sparkassen werfen ihnen vor, grob fahrlässig gehandelt zu haben, wenn sie beispielsweise auf einen Anruf eines angeblichen Bankmitarbeiters eingegangen sind oder eine Phishing-Mail angeklickt haben. Sie unterstellen dabei, dass Betrug relativ leicht zu erkennen sei. Doch ist das wirklich der Fall?

ZUSAMMENFASSUNG

Zwischen 1. und 4. November 2023 wurden in einer internetnutzerrepräsentativen Online-Befragung Teilnehmer:innen mit Abläufen oder E-Mails aus dem Zahlungsverkehr oder der digitalen Welt konfrontiert. Die Hälfte der dargestellten Fallsituationen simulierte einen betrügerischen Angriff auf die Zahlungskonten der Betroffenen. Die andere Hälfte hingegen waren Kommunikationsbeispiele und Prozesse, wie sie tatsächlich von echten Anbietern am Markt ohne betrügerischen Hintergrund durchgeführt wurden. Die Teilnehmer:innen wurden befragt, wie sie die jeweilige Situation einschätzen und wie sie darauf reagieren würden.

Die betrügerischen Angriffe und das echte Anbieterverhalten waren für die Befragten schwer zu differenzieren. Bei den betrügerischen Fallkonstellationen äußerten 57 Prozent der Befragten einen Betrugsverdacht, allerdings auch bei 38 Prozent der Fallkonstellationen mit einem nicht betrügerischen Anbieterverhalten. 24 Prozent waren sich im Fall der Angriffe über die betrügerischen Absichten so sicher, dass sie es komplett ablehnten, auf das Anliegen einzugehen. Dies traf aber auch auf 19 Prozent der echten Anbieterverhaltensweisen zu.

Warnmeldungen, die Anbieter in der Regel versenden, um Verbraucher:innen zum Beispiel auf die Übernahme eines Authentisierungsinstruments im Zuge eines Betrugs hinzuweisen, waren so schlecht gestaltet, dass nur 16 Prozent derjenigen, die auf den Betrug hereingefallen waren, den Betrug daraufhin erkannten. Andere sahen in diesen Warnmeldungen im Gegenteil gerade eine Bestätigung ihres richtigen Handelns und wogen sich in falscher Sicherheit.

43 Prozent der Teilnehmer:innen, die in der Befragungssituation auf den Betrug hereingefallen waren, gaben an, dass sie in der Konsequenz massive Einschränkungen in ihrem Verhalten vornehmen würden: Sie würden nicht mehr im Internet bezahlen, kein Online-Banking mehr machen oder ihr digitales Leben stärker einschränken.

Diejenigen, die den Betrugsversuch während der Befragung erkannten, identifizierten diesen am häufigsten an typischen Betrugsmerkmalen wie einer auffälligen E-Mail-Adresse, Aufbauen von Druck und Dringlichkeit oder einem verdächtigen Link in der Nachricht. Am zweithäufigsten wurde aber angegeben, dass sie aufgrund eines allgemeinen Eindrucks oder eines Misstrauens zu ihrer Erkenntnis kamen.

Bei den echten, nicht betrügerischen Anbieterverhalten kritisierten die Teilnehmer:innen unter anderem, dass die Prozesse oder Nachrichten unverständlich, kompliziert oder verwirrend seien. Es ist somit zu vermuten, dass Verbraucher:innen im normalen Zahlungsverkehr teilweise lernen, Prozessen zu folgen, die sie nicht komplett verstehen.

Auf Grund der Ergebnisse erscheint dem vzbv schließlich der von Anbieterseite immer wieder vorgebrachte Vorwurf an Verbraucher:innen, dass sie durch Eingehen auf eine betrügerische Nachricht grob fahrlässig gehandelt hätten, eher unwahrscheinlich. Denn dies würde die zuverlässige Erkennbarkeit von Betrug in diesem Zusammenhang voraussetzen.

I. HINTERGRUND

Das Geld der Verbraucher:innen ist zunehmend im Fokus von Kriminellen. Mit Phishing-Mails, Spoofing-Anrufen und Links zu gefälschten Webseiten versuchen Betrüger:innen an Bankkonten und Zahlungskarten zu gelangen. Bei dieser mit „Social Engineering“ bezeichneten Angriffsmethode sind die Verbraucher:innen selbst das Ziel der Angreifer:innen. Im Jahr 2022 enthielten fast 70 Prozent aller Spam-Mails Cyber-Angriffe. Und neun von zehn der betrügerischen Mails täuschten vor, von einer Bank oder Sparkasse zu stammen.[1] Im Jahr 2023 hat diese Form des Betrugs nicht nur erheblich an Dynamik gewonnen, sondern verursachte auch höhere Schadenssummen bei gleichzeitig sinkender Aufklärungsquote.[2] Die Beschwerdestatistik der Verbraucherzentralen verzeichnete im Jahr 2023 im Vergleich zum Vorjahr eine Verdoppelung der Verbraucherbeschwerden zu Cyberkriminalität im Zusammenhang mit Finanzdienstleistungen.[3] Dabei wenden sich Verbraucher:innen in der Regel nur dann an die Verbraucherzentralen, wenn ihre Bank oder Sparkasse Schäden zunächst nicht reguliert und die Geschädigten auf dem Verlust sitzen bleiben. Dies untermauerte auf gesamteuropäischer Ebene auch die Europäische Bankenaufsicht EBA im Jahr 2022: Sie stellte fest, dass Verbraucher:innen bei betrügerischen Kontoabbuchungen und Geldabhebungen in etwa zwei Dritteln der Fälle den Schaden selbst tragen mussten.[4]

Die Europäische Union indessen hatte mit der Richtlinie 2015/2366 festgeschrieben, dass Verbraucher:innen in derartigen Fällen von Cyberkriminalität in der Regel gerade nicht haften.[5] Sie tragen auch nicht die Beweislast, da „im Falle von Online-Zahlungen, […] die entsprechenden Möglichkeiten des Zahlers […] sehr begrenzt sind“.[6] Es gibt nur zwei Ausnahmen, bei denen Verbraucher:innen in voller Höhe selbst haften: Wenn sie selbst betrügen oder grob fahrlässig handeln. Grob fahrlässig zu handeln bedeutet im Allgemeinen einen besonders schweren Verstoß gegen die objektiv erforderliche

[1] Beller, Tanja: Cyberangriffe auf Bankkunden - aktuelle Betrugsmaschen, 2023, https://bankenverband.de/cyberkriminalitaet/cyberangriffe-auf-bankkunden-das-sind-die-aktuellen-betrugsmaschen/, 06.07.2023.

[2] Kirchner, Christian: Warum Kartenbetrug für unsere Banken ein massives Problem ist, 2023, https://finanz-szene.de/payments/warum-kartenbetrug-fuer-unsere-banken-neuerdings-ein-massives-problem-ist/, 26.01.2024.

[3] Die Auswertungen der Beschwerdestatistik basieren auf der Vorgangserfassung aller 16 Verbraucherzentralen in den insgesamt rund 200 Beratungsstellen in Deutschland. Die Vorgangserfassung stellt die statistische Erfassung aller Verbraucheranliegen dar, die an die Verbraucherzentralen herangetragen werden. Direkte Rückschlüsse auf die Häufigkeit des Vorkommens bestimmter Verbraucherprobleme in der Gesamtbevölkerung sind daraus jedoch nicht ableitbar. Die Beschwerden, welche die Verbraucherzentralen erreichen, repräsentieren nur einen Bruchteil der tatsächlich verärgerten Verbraucher:innen, da sich nicht alle Betroffenen an ihre Verbraucherzentrale wenden. Aufgrund einer Anpassung des Erfassungsprozesses zum Jahreswechsel 2022/23 sind die Beschwerdezahlen der VZ Baden-Württemberg (BW) nicht mit denen vor diesem Zeitpunkt vergleichbar. Deshalb ist BW bei dieser Datenauswertung nicht berücksichtigt. Ausgewählte Beschwerdegründe: „Phishing“ / „nicht autorisierte Kontoabbuchungen“ / „Identitätsdiebstahl“. Die Gesamtanzahl der Beschwerden lag im Jahr 2023 im niedrigen vierstelligen Bereich.

[4] European Banking Authority: Discussion Paper on the EBA’s preliminary observations on selected payment fraud data under PSD2, as reported by the industry, 2022, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/discussion-paper-payment-fraud-data-received-under-psd2, 11.08.2023.

[5] Europäische Union: Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32015L2366, 26.01.2024.

[6] Ebd., Erwägungsgrund 72.

Sorgfalt, was letztlich heißt, ohne die geringste Vorsicht und Aufmerksamkeit zu handeln. Genau dies werfen Banken und Sparkassen geschädigten Verbraucher:innen regelmäßig vor.[7]

Seltsame Buchungen auf fremde Konten, teilweise mehrere hintereinander und in ungewöhnlich hohen Beträgen hätten die Verbraucher:innen, so die wiederkehrenden Argumentationen der Anbieter, selbst autorisiert. Schließlich sei der Vorgang technisch korrekt freigegeben worden. Und „da der Code nicht an Dritte weitergegeben werden darf, kann die […] App nur auf Ihrem mobilen Endgerät aktiviert worden sein“ (aus einem Schreiben der DKB). Ähnlich ein anderer Anbieter: „Für Belastungen auf Ihre[n] Kreditkarten [werden] sensible Daten benötigt, welche ausschließlich Ihnen als Karteninhaber bekannt sein können“ (aus einem Schreiben der BW Bank). Somit gebe es „keinen Hinweis darauf, dass die Aufträge nicht durch Sie erteilt wurden“ (aus einem Schreiben der Postbank), denn „bei Einhaltung der vertraglich vereinbarten Sorgfaltspflichten ist ein Kartenmissbrauch durch Dritte ausgeschlossen“ (aus einem Schreiben der DKB). Sollten Verbraucher:innen betrogen worden sein und vermeintliche Freigaben erteilt haben, die sie gar nicht wünschten, scheint den Anbietern und den Schlichtungsstellen die Lage klar:

- „Die Weitergabe der Authentifizierungselemente stellt entsprechend der Bedingungen für die VISA Card eine grob fahrlässige Verletzung der Sorgfaltspflichten dar.“ (aus einem Schreiben der ING)
- „Im Hinblick auf die Sorgfaltspflichten […] zum Schutz der Authentifizierungselemente bei der Nutzung des Online-Banking, sowie die Beachtung der Sicherheitshinweise auf der Online-Banking Seite der Bank […] erachten wir die Handlungsweise […] für grob fahrlässig.“ (aus einem Schreiben der Sparda-Bank Südwest)
- „Alle betrügerischen Verfügungen sind […] nur erklärbar, wenn Sie personalisierte Sicherheitsmerkmale […] weitergegeben oder eingegeben haben. Dies stellt einen grob fahrlässigen Verstoß gegen die Sorgfaltspflichten im Online-Banking dar.“ (aus einem Schreiben der Ostsee-Sparkasse Rostock)
- „Der Anfrage der Neuregistrierung von Apple Pay auf einem mobilen Endgerät haben Sie nachweislich zugestimmt und daher grob fahrlässig gehandelt.“ (aus einem Schreiben der Landesbank Berlin)
- „Wir warnen in den aktuellen Sicherheitswarnungen auf unserer Homepage ausdrücklich vor Betrugsversuchen. Die Beachtung dieser Hinweise ist Voraussetzung für sicheres Online-Banking. Leider scheinen Sie dies nicht berücksichtigt zu haben.“ (aus einem Schreiben der Postbank)
- „Das Durchführen der verlangten ‚Sicherheitsabfrage‘ auf einer nicht selbst aufgerufenen, sondern per Link übermittelten Internetseite stellt eine grob fahrlässige Verletzung der Pflicht […] dar.“ (aus einem Schlichtungsspruch des Ombudsmanns für den Deutschen Sparkassen- und Giroverband)

Anbieter behaupten also, betrügerische Buchungen, die unter Vorspiegelung falscher Tatsachen und mit hoher krimineller Energie und teils erheblichem technischem Aufwand erschlichen wurden, seien ordnungsgemäß autorisiert worden. Und wenn Verbraucher:innen dabei nicht gemerkt hätten, dass sie Betrüger:innen aufsitzen, hätten

[7] Siehe Verbraucherzentrale Bundesverband: Verbraucherprobleme bei betrügerischen Kontozugriffen, 2022, https://www.vzbv.de/sites/default/files/2022-11/2022-09-28_Unautorisierte-Verfuegungen.pdf, 26.01.2024.

sie gegen die AGB verstoßen, wahlweise auch Sicherheitshinweise auf den Internetseiten der Banken missachtet und damit grob fahrlässig, also ohne die geringste Vorsicht und Aufmerksamkeit gehandelt. Doch ist es wirklich so einfach, Betrug zu identifizieren, Phishing-Mails zu erkennen und nicht auf gefälschte Webseiten hereinzufallen? Passiert das nur, wenn ohne jegliche Vorsicht und Aufmerksamkeit, also grob fahrlässig gehandelt wird? Diesen Fragen ging die Marktbeobachtung des vzbv in einer Studie nach.

II. WIE WURDE UNTERSUCHT?

Vom 1. bis zum 4. November 2023 erhielten 1.035 Teilnehmer:innen in einer internetnutzerrepräsentativen Online-Befragung jeweils vier unterschiedliche Fallsituationen aus der digitalen Welt bzw. dem Zahlungsverkehr präsentiert und sollten diese einschätzen. Außerdem wurden sie gefragt, wie sie darauf reagieren würden.[8] Unter den vier Situationen gab es jeweils eine Konstellation pro Teilnehmer:in, mit der sich Betrüger:innen Zugriff auf das Konto verschaffen würden. Außerdem umfasste die Befragung jeweils eine weitere Konstellation, die einem echten, nicht betrügerischen Verhalten eines Anbieters entsprach. Die übrigen zwei Konstellationen wurden aus rein methodischen Gründen in die Befragung integriert und hatten keine inhaltliche Relevanz für die Erhebung.

Über alle Befragten hinweg wurden insgesamt zehn unterschiedliche betrügerische Konstellationen bzw. zehn echte, nicht betrügerische Verhaltensweisen von Anbietern überprüft, sodass jede Konstellation von mindestens 100 Befragten beurteilt wurde. Die ausgewählten Fallkonstellationen entstammten den Dokumentationen im Frühwarnnetzwerk der Verbraucherzentralen und des vzbv[9], der Sammlung des Phishing-Radars der Verbraucherzentrale Nordrhein-Westfalen sowie eigenständig durchgeführten Dokumentationen der Marktbeobachtung des vzbv.

Bei der Auswahl der betrügerischen Konstellationen wurde darauf geachtet, dass Phishing-Angriffe in unterschiedlich guter Qualität in der Studie abgebildet waren. So umfassten die überprüften Fallkonstellationen Phishing-Versuche, die vollkommen unpersonalisiert waren und die gut sichtbar von dubiosen E-Mail-Absendern stammten. Gleichermaßen waren aber auch personalisierte E-Mails mit getarnten Absenderadressen enthalten und in einem Fall auch mit weiteren persönlichen Daten (hochpersonalisiert), wie sie etwa aus der immer größer werdenden Anzahl an Datenlecks[10] oder aufgrund fehlerhafter Konfigurationen von IT-Systemen[11] entstammen können. Jeweils eine Konstellation bildete einen Smishing-Angriff, also per SMS-Nachricht, und eine Pharming-Seite, also eine gefälschte Webseite, ab. In vier Fällen wurde die Situation

[8] Die Erhebung führte eye square GmbH im Auftrag von und nach einem Konzept des vzbv durch. Statistische Fehlertoleranz: max. ± 3 Prozentpunkte in der Gesamtstichprobe.

[9] Beim Frühwarnnetzwerk der Verbraucherzentralen und des vzbv (FWN) handelt es sich um ein qualitatives Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung. Grundlage stellt eine ausführliche Sachverhaltsschilderung durch Beratungskräfte dar, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht. Eine Quantifizierung der Daten aus dem FWN heraus bzw. ein Rückschluss auf die Häufigkeit des Vorkommens in der Verbraucherberatung oder in der Gesamtbevölkerung insgesamt ist daher nicht möglich.

[10] Siehe Datenlecks ernstzunehmende Bedrohung der Cyber-Sicherheit der gesamten FSI-Branche, 2023, https://www.datensicherheit.de/datenlecks-ernst-bedrohung-cyber-sicherheit-fsi-branche, 24.08.2023.

[11] Siehe beispielsweise Shabaviz, Mario: Gravierende Sicherheitslücken bei Sparkassen, 2023, https://www.zdf.de/nachrichten/ratgeber/sparkasse-online-banking-zwei-faktor-authentifizierung-100.html, 09.02.2024.

nachgestellt, dass sich betrügerische Angriffe gezielt an Prozesse anlehnen, die die echten Anbieter zu dem Zeitpunkt tatsächlich gerade durchführen, zum Beispiel eine Umstellung der ausgegebenen Zahlungskarten. Dies ist nach Erkenntnissen des vzbv regelmäßig zu beobachten und macht die Angriffe besonders gefährlich.[12] Im Zuge der Bearbeitung hatten die Befragten die Möglichkeit, Prüfungen beispielsweise der tatsächlich verlinkten Ziel-URLs oder der Absenderadressen per Mouseover vorzunehmen oder auch den Aussteller eines Sicherheitszertifikats anzusehen.

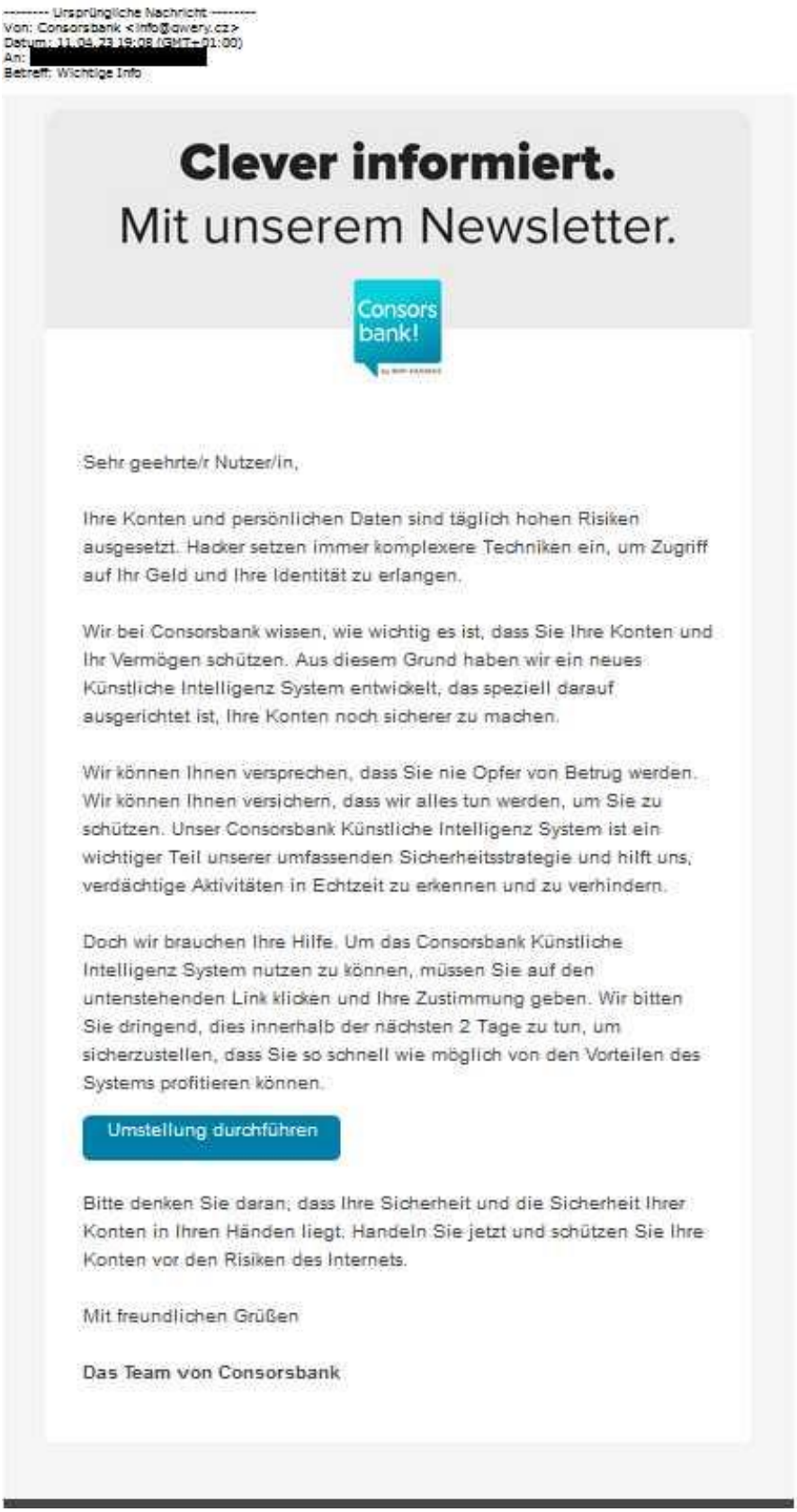
Die Fallkonstellationen bilden einen Querschnitt üblicher Angriffsversuche ab, wie sie in Massenmails täglich Verbraucher:innen erreichen. Gezielt platzierte Angriffe (Spear-Phishing) wurden dagegen nicht geprüft.

Tabelle 1: Betrügerische Fallkonstellationen

Überprüfte betrügerische Fallkonstellationen:
1. Forderung einer nachträglichen Gebührenzahlung nach Warenbestellung
2. Widerspruch gegen eine Kündigung von Zahlungskarten (Andocken an echten Prozess)
3. Umsetzung europäischer Sicherheitsnormen
4. Widerspruch gegen die Deaktivierung eines Kontos (hochpersonalisiert)
5. Datenüberprüfung wegen Geldwäscheprävention
6. Umstellung des Onlinebanking-Systems (Smishing, Andocken an echten Prozess)
7. Bezahlung nach Warenbestellung (Pharming)
8. Aktualisierung von Nutzungsbedingungen (Andocken an echten Prozess)
9. Werbung für neues, sichereres TAN-Verfahren (Andocken an echten Prozess)
10. Werbung für KI-gesichertes Banking-System

[12] Siehe beispielsweise Gerbig, Gerrit: Postbank-Phishing: Kriminelle nutzen Neujahrsumstellung aus, 2023, https://www.netzwelt.de/news/212139-postbank-phishing-betrueger-nutzen-neujahrsumstellung.html, 09.02.2024; Pieper, Marco: Neue Phishing-Welle: "Bestätigen Sie per QR-Code die neue AGB Ihrer Bank" ist Spam, 2021, https://www.netzwelt.de/news/193263-neue-phishing-welle-bestaetigen-per-qr-code-neue-agb-ihrer-bank-spam.html, 09.02.2024.

Grafik 1: Beispiel einer in der Studie verwendeten Phishing-Nachricht



--------- Ursprüngliche Nachricht ---------
Von: Consorsbank <info@qwery.cz>
Datum: 11.09.23 19:08 (GMT+01:00)
An: [redacted]
Betreff: Wichtige Info

Clever informiert.
Mit unserem Newsletter.

Consors bank!

Sehr geehrte/r Nutzer/in,

Ihre Konten und persönlichen Daten sind täglich hohen Risiken ausgesetzt. Hacker setzen immer komplexere Techniken ein, um Zugriff auf Ihr Geld und Ihre Identität zu erlangen.

Wir bei Consorsbank wissen, wie wichtig es ist, dass Sie Ihre Konten und Ihr Vermögen schützen. Aus diesem Grund haben wir ein neues Künstliche Intelligenz System entwickelt, das speziell darauf ausgerichtet ist, Ihre Konten noch sicherer zu machen.

Wir können Ihnen versprechen, dass Sie nie Opfer von Betrug werden. Wir können Ihnen versichern, dass wir alles tun werden, um Sie zu schützen. Unser Consorsbank Künstliche Intelligenz System ist ein wichtiger Teil unserer umfassenden Sicherheitsstrategie und hilft uns, verdächtige Aktivitäten in Echtzeit zu erkennen und zu verhindern.

Doch wir brauchen Ihre Hilfe. Um das Consorsbank Künstliche Intelligenz System nutzen zu können, müssen Sie auf den untenstehenden Link klicken und Ihre Zustimmung geben. Wir bitten Sie dringend, dies innerhalb der nächsten 2 Tage zu tun, um sicherzustellen, dass Sie so schnell wie möglich von den Vorteilen des Systems profitieren können.

Umstellung durchführen

Bitte denken Sie daran, dass Ihre Sicherheit und die Sicherheit Ihrer Konten in Ihren Händen liegt. Handeln Sie jetzt und schützen Sie Ihre Konten vor den Risiken des Internets.

Mit freundlichen Grüßen

Das Team von Consorsbank

Die Auswahl der echten, nicht betrügerischen Fallkonstellationen umfasste Werbeangebote oder auch die Einführung neuer Systeme. Außerdem wurden echte Prozesse

im Onlinebanking oder die Einrichtung neuer Authentisierungsverfahren abgebildet. Weiterhin umfassten diese Konstellationen Überprüfungen, die Anbieter durchführten, um die Echtheit des Kundenverhaltens zu verifizieren, und zuletzt auch die Einbindung von Bankkonten in Kontoinformationsdiensten. Zwei der aufgenommenen Konstellationen bildeten einen Prozess ab, dessen konkreter Ablauf vermutlich vom intendierten Ablauf abwich. Hier erfolgten beispielsweise überraschende Fehlermeldungen im Prozess oder es wurde für weitere Prozessschritte eine TAN gefordert, deren tatsächliche Eingabe aber keine Auswirkungen auf den Prozess hatte.

Tabelle 2: Nicht betrügerische Fallkonstellationen

Überprüfte echte Fallkonstellationen:
A. Einloggen ins Onlinebanking und Ausführen einer Überweisung (Prozess, vermutlich nicht intendiert: Eingegebene TAN erzeugt keine Wirkung)
B. Werbung für neues Onlinebanking
C. Einrichtung eines neuen Authentisierungsverfahrens (Prozess)
D. Verifizierungsmail zum Kundenverhalten (Prozess)
E. Werbung für komfortableres Trading
F. Werbung für neues Onlinebanking
G. Bestätigung eines Zahlungsverkehrskontos in Versandhandelsplattform (Prozess)
H. Werbung für sichereres Browsing im WWW
I. Einbindung eines Bankkontos in Kontoinformationsdienst (Prozess)
J. Einbindung eines Bankkontos in Kontoinformationsdienst (Prozess, vermutlich nicht intendiert: Nach erfolgter Einbindung erscheint Fehlermeldung)

Da ein Betrugsverdacht in einer Befragung aus methodischen Gründen nicht direkt abgefragt werden kann, wurde dieser indirekt erhoben und dafür folgendes Vorgehen gewählt: Die Befragten wurden zunächst immer über ein Freitextfeld nach ihrem ersten Eindruck zu der zuvor präsentierten Konstellation befragt. Anschließend erhielten sie in der Regel[13] vier Auswahloptionen, wie sie sich in dieser Situation verhalten würden. Sie konnten angeben, (1) dass sie das Anliegen nicht gleich erledigen, dies aber später tun wollen (d. h. im obigen Beispiel aus Grafik 1: Wechseln zum neuen System durch Klick auf „Umstellung durchführen“), (2) dass sie das Anliegen sofort erledigen werden, (3) dass sie nicht auf das Anliegen eingehen werden und (4) dass sie zunächst eine dritte Person (Bekannte, Experten, Berater) kontaktieren wollen. Diese vier Antwortoptionen wurden durch ein „Sonstiges“-Feld ergänzt, um ein in den vier Optionen nicht enthalte-

[13] Eine Ausnahme bildete Fallkonstellation A: Hier wurde die Eingabe eines Passworts verlangt. Befragte konnten auswählen, es entweder einzugeben oder es nicht einzugeben.

nes Verhalten als offene Antwort in Textform dokumentieren zu können. Aus dem Gesamteindruck aller geschlossenen und offenen Antworten wurde für jede Konstellation und jede befragte Person nachträglich codiert, ob die jeweils Befragten (1) auf das Anliegen eingehen, (2) wegen eines Betrugsverdachts nicht auf das Anliegen eingehen, (3) trotz keines geäußerten Betrugsverdachts nicht auf das Anliegen eingehen, (4) in einer anderen Weise handeln oder (5) das abschließende Handeln nicht beurteilt werden kann, zum Beispiel weil die Befragten noch nicht alle Informationen vorliegen hatten, die sie für die Beurteilung wünschten. D. h. im Nachgang wurde codiert, ob die Befragten in der jeweiligen Situation einen Betrugsverdacht hegten. Nachfolgend dargestellt ist jeweils ein Beispiel für jede dieser nachträglichen Klassifikationen:

Tabelle 3: Beispiele für Nachcodierungen der Antworten

Antwort auf Frage: Was denken Sie? (Freitext)	**Antwort auf Frage: Was tun Sie?**	**Antwort auf Frage nach Begründung (Freitext)**	**Nachcodierte Bewertung**
„Verständlich, da Sicherheit gewährleistet wird.“	„Ich erledige es gleich und schalte das Banking über den Link wieder frei.“		(1) Eingehen auf Anliegen
„Diese E-Mail kommt sicher nicht von der Bank.“	„Ich bespreche die Sache mit einer nahestehenden Person, einem Experten oder einem Mitarbeiter der Bank.“	„Ich würde tatsächlich als erstes einen Mitarbeiter dieser Bank kontaktieren um zu erfragen, ob diese E-Mail aus deren Haus stammt.“	(2) kein Eingehen auf Anliegen wegen Betrugsverdachts
„Ich finde die schärferen Sicherheitsabfragen übertrieben. Besonders für ältere Menschen fast schon nicht zumutbar.“	„Ich bespreche die Sache mit einer nahestehenden Person, einem Experten oder einem Mitarbeiter der Bank.“	„Ich vertraue den KI-gesteuerten Prozessen nicht.“	(3) kein Eingehen auf Anliegen, obwohl kein Betrugsverdacht
„Aus Sicherheitsgründen nicht verkehrt.“	„Sonstiges“	„Ich schließe die Mail und gehe direkt auf die Bankseite.“	(4) anderes Handeln
„Ich würde bei der Bank anrufen.“	„Sonstiges“	„Ich rufe an.“	(5) nicht beurteilbar

III. ERGEBNISSE

1. BETRÜGERISCHE FALLKONSTELLATIONEN

Nach Auswertung der betrügerischen Fallkonstellationen war festzustellen, dass die große Mehrheit nicht auf die Betrugsmaschen hereinfallen würde. Nur 21 Prozent der Befragten gaben auf die Frage, was sie tun würden, ihre Bereitschaft an, auf die dargestellten Anliegen einzugehen. Immerhin 12 Prozent darunter empfanden das jeweilige Anliegen als so dringend, dass sie dies auch umgehend getan hätten. Demgegenüber lehnten es 31 Prozent der Befragten grundsätzlich ab, auf das Anliegen einzugehen.[14]

Von den Personen, die angaben, grundsätzlich nicht auf das Anliegen einzugehen, begründeten dies zudem nicht alle, sondern nur 77 Prozent (dies entspricht 24 Prozent aller Befragten, die eine betrügerische Fallkonstellation erhielten) mit einem konkreten Betrugsverdacht.[15] Die übrigen gaben beispielsweise bei Fallkonstellation 1 (Forderung einer nachträglichen Gebührenzahlung nach Warenbestellung) an, dass sie nicht zahlen würden, weil die geforderten Gebühren vorher nicht vereinbart waren oder weil ihnen die Gebühren zu intransparent dargestellt waren. Bei Fallkonstellation 2 (Widerspruch gegen eine Kündigung von Zahlungskarten) gaben Befragte beispielsweise als Begründung für ihre Ablehnung an, dass sie grundsätzlich nicht damit einverstanden seien, dass die neue Karte kostenpflichtig werde oder dass die E-Mail zu wenig Informationen enthalte. Bei Fallkonstellation 3 (Umsetzung europäischer Sicherheitsnormen) wären Befragte beispielsweise deshalb nicht auf das Anliegen eingegangen, weil sie gegenüber dem angepriesenen Einsatz von Künstlicher Intelligenz grundlegend skeptisch sind.

Knapp die Hälfte der Teilnehmer:innen (48 Prozent) ging weder (sofort) auf die betrügerischen Fallkonstellationen ein, noch lehnten sie dies grundsätzlich ab (siehe hierzu Detailergebnisse Fußnote 14). In dieser Befragtengruppe äußerten jedoch weitere 68 Prozent einen Betrugsverdacht.[16] Da sie sich aber nicht ganz sicher waren, zogen sie es vor, sich zunächst mit einer dritten Person zu besprechen oder mittels eines sonstigen Vorgehens eine Klärung herbeizuführen.

Unabhängig von ihrer ersten Handlung äußerten somit letztlich insgesamt 57 Prozent der Befragten, die eine betrügerische Fallkonstellation bewerten sollten, einen konkreten Betrugsverdacht.[17] Nur 24 Prozent darunter waren sich mit ihrer Einschätzung jedoch so sicher, dass sie es sofort ablehnten, auf die betrügerische Aufforderung der jeweiligen Fallkonstellation einzugehen. [18]

---

[14] Ergebnisse im Detail: 9 Prozent erledigen Anliegen nicht gleich, aber später; 12 Prozent erledigen es sofort (= 21 Prozent, die insgesamt auf das Anliegen eingehen); 31 Prozent gehen nicht auf das Anliegen ein; 35 Prozent besprechen sich zunächst mit dritter Person; 13 Prozent wählen ein sonstiges Vorgehen. Basis: 1.035 Befragte. Kumulierte Werte über alle zehn betrügerischen Fallkonstellationen

[15] Basis: Befragte, die angaben, grundsätzlich nicht auf das Anliegen einzugehen, bzw. alle Befragten

[16] Basis: Befragte, die weder auf das Anliegen eingingen noch es (direkt) ablehnten

[17] Basis: 1.035 Befragte. Kumulierte Werte über alle zehn betrügerischen Fallkonstellationen

[18] Basis: Befragte, die einen Betrugsverdacht äußerten

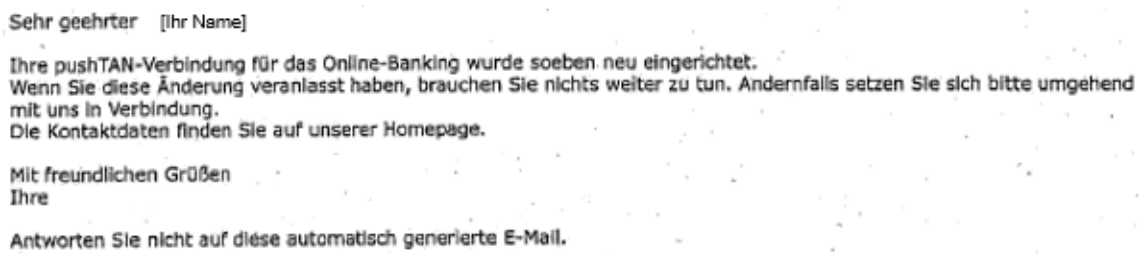
2. VARIATIONEN DER BETRUGSMAILS

In der Hälfte der Fallkonstellationen wurde eine höhere betrügerische Qualität dadurch erzeugt, dass sie entweder an tatsächliche Prozesse der jeweiligen Anbieter angelehnt waren oder über die reine Namensansprache hinaus zusätzliche Personalisierungsmerkmale enthielten. Vor allem letztere Gestaltung erfordert für Betrüger:innen mehr Aufwand bei der Erstellung. Im Ergebnis aber waren diese Betrugsmails auch potenziell gefährlicher. 25 Prozent der Befragten wären auf diese Anliegen eingegangen. Bei den Mails von geringerer Qualität traf dies dagegen nur auf 17 Prozent zu. Außerdem äußerten weniger Befragte bei diesen Mails den Verdacht, dass es sich um Betrug handeln könnte. Angesichts immer ausgefeilterer Angriffstechniken und der auch durch den Einsatz von Künstlicher Intelligenz stetig zunehmenden Qualität von Betrugsmails bei gleichzeitig sinkenden Kosten[19] für die Betrüger:innen ist nach Auffassung des vzbv davon auszugehen, dass die ohnehin schon steigende Quote immer erfolgreicherer Angriffe auch in Zukunft weiter steigen wird.

3. WARNMELDUNGEN

Ein für Betrüger attraktives Angriffsziel ist die Übernahme der Authentisierungsinstrumente von Verbraucher:innen. Die Betrüger sind dann in der Lage, selbstständig beliebige Transaktionen vom gekaperten Konto auszuführen, ohne dass eine weitere Mithilfe der Kontoinhaber:innen erforderlich ist. Um ihre Kund:innen auf die Übernahme von Authentisierungsinstrumenten hinzuweisen, versenden Anbieter in der Regel entsprechende SMS oder E-Mail-Nachrichten an die Kontoinhaber:innen. Bei den betrügerischen Fallkonstellationen 2 und 3 wurden die Befragten, die nicht angegeben hatten, dass sie auf das Anliegen auf keinen Fall eingehen würden, im weiteren Verlauf mit solchen Warnnachrichten konfrontiert.

Grafik 2: Beispiel des Textes einer Warnmeldung



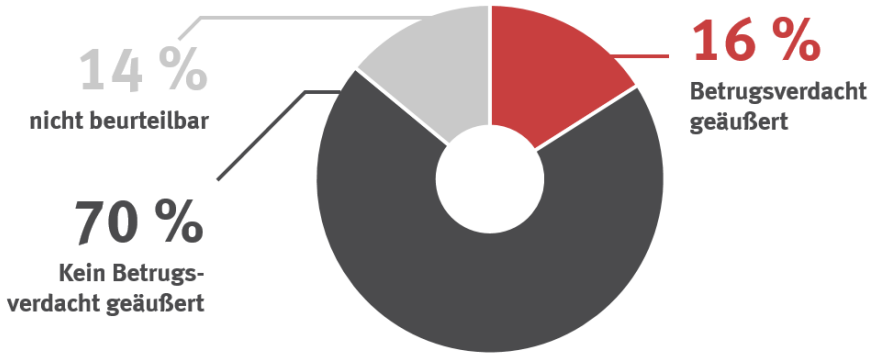
Analog zu den zuvor erhaltenen Betrugsmails wurden die Teilnehmer:innen auch hier dazu befragt, was sie darüber dächten. Außerdem wurden sie in einer Folgefrage mit verschiedenen Aussagen konfrontiert, von denen sie eine oder mehrere auswählen oder eine selbstformulierte Aussage hinzufügen konnten.

In Konstellation 2 gaben nur 15 von 45 Befragten an, dass sie aufgrund dieser Warnmeldung ihre Bank kontaktieren würden. Neun von 45 gaben immerhin an, dass sie mit einer nahestehenden Person darüber sprechen würden. In Konstellation 3 äußerten 36 der 74 Befragten, ihre Bank kontaktieren zu wollen; und acht der 74 wollten die Nach-

[19] Ein Team von IBM X-Force hat 2023 innerhalb von fünf Minuten mit nur fünf Prompts sehr überzeugende Phishing-Mails allein mit KI erzeugt, also gänzlich ohne menschliche Kreativität (Carruthers, Stephanie: AI vs. human deceit: Unravelling the new age of phishing tactics, 2023, https://securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics/, 18.03.2024).

richt einer nahestehenden Person zeigen. Die Abweichung zwischen den beiden Fallkonstellationen lässt die Vermutung zu, dass die Qualität dieser Warnmeldungen von Anbieter zu Anbieter sehr unterschiedlich sein kann. Tatsächlich gibt es keinen Standard, wie eine derartige Nachricht aussehen muss oder wie sie zu übermitteln ist.

Grafik 3: Folgen nach Erhalt der Warnmeldung



Über die beiden Fallkonstellationen mit Warnmeldungen hinweg wurde das Ziel dieser Warnungen im Großen und Ganzen verfehlt. Einen konkreten Betrugsverdacht äußerten infolge dieser Warnmeldung lediglich 16 Prozent der Befragten. 70 Prozent hingegen äußerten keinen Betrugsverdacht.[20] Die Mehrheit der Teilnehmer:innen hat den Inhalt somit nicht korrekt verstanden. So gaben Befragte unter anderem an, dass sie es als normale Bestätigung ihres zuvor aufgrund der Betrugsmail veranlassten Handelns sahen. Sie sahen sich also im Erhalt dieser E-Mail gerade darin bestätigt, dass alles korrekt ablief und kein Betrug war, wie an folgenden Kommentaren deutlich wird:

> „Das ist ein übliches Vorgehen und dient meiner Sicherheit“; „Es scheint eine sichere Vorgehensweise zu sein“; „Super, alles hat geklappt“; „Nichts Besonderes, das Vorgehen wirkt normal“; „Ich finde es gut, dass ich nochmals eine Nachricht bekomme, wenn ich etwas an meinem Online-Banking verändert habe. Dies vermittelt eine große Sicherheit“; „Standard Benachrichtigung, die ich erwarte, wenn ich Änderungen vorgenommen habe“; „Eine extra Sicherheitsstufe ist immer gut, ich muss nicht auf die E-Mail reagieren, solange ich selbst die neue Einrichtung vorgenommen habe“.

Andere Teilnehmer:innen kommentierten aber auch, dass der Inhalt der Warnmeldung nicht ganz verständlich wird:

> „Ich finde es verwirrend, dass es in der Mail keine Information zum Status meiner Visakarte gibt“; „Ist für mich verwirrend“; „Unverständlich“; „Schon bekannt, für ältere Kunden nicht zu verstehen!“

Die Warnmeldungen, die Anbieter versenden und auf die sie sich immer wieder berufen, wenn sie Verbraucher:innen grobe Fahrlässigkeit vorwerfen, sind also so schlecht verständlich, dass die Mehrheit der Teilnehmer:innen deren Inhalt nicht korrekt erfasst hat bzw. sie im Gegenteil als Bestätigung ihres korrekten Verhaltens betrachtete. Einzelne Befragte hatten sogar genau diese Warnmeldung im Verdacht, betrügerisch zu sein.

[20] Bei den verbleibenden Befragten ließen die Freitexte keine eindeutige Schlussfolgerung zu. Basis: Befragte, die eine Warnmeldung erhalten haben

4. GRÜNDE FÜR BETRUGSVERDACHT

Personen, die bei den betrügerischen Fallkonstellationen nicht auf den Betrug hereingefallen waren, weil sie es entweder grundsätzlich ablehnten, auf das Anliegen einzugehen, oder sich zunächst mit einer dritten Person besprechen wollten, wurden am Ende nach den Gründen hierfür gefragt. Hierbei konnten mehrere Gründe genannt werden. Zur Auswertung wurden nur die Antworten der Personen herangezogen, die tatsächlich einen Betrugsverdacht geäußert hatten.

Die Befragten nannten hierbei in der Summe am häufigsten klassische Phishing-Merkmale wie eine auffällige E-Mail-Adresse, einen verdächtigen Link in der Nachricht, Aufbauen von Druck und Dringlichkeit, eine fehlende persönliche Anrede, einen verdächtigen Inhalt der Nachricht oder die Art und Weise des Kontaktaufbaus. Der am zweithäufigsten genannte Grund war aber ein allgemeiner Eindruck bzw. ein Misstrauen gegenüber dem Vorgehen oder dem vermeintlichen Unternehmen. Diese Befragten begründeten den Verdacht unter anderem wie folgt: „Die Aufmachung der Mail erscheint mir sehr suspekt“, „Die E-Mail sieht nicht echt aus.“, „Die ganze Art der E-Mail hat mich aufhorchen lassen.“, „Es ist heutzutage gut möglich, sowas zu fälschen und echt aussehen zu lassen“, „da ich nicht sicher war, ob es eine Fakenachricht ist“, „alles schlecht“, „Der ganze Vorgang. Warum sollte ich auf einmal irgendwelche Gebühren bezahlen?“

Die Ergebnisse zum Themenbereich Betrugsverdacht zeigten somit, dass die Befragten, die nicht auf den Betrug hereinfielen, die Täuschung aufgrund von zwei Methoden entlarvten: zum einen aufgrund ihres Wissens über typische Merkmale von Betrugsnachrichten, zum anderen aber auch aufgrund ihrer allgemeinen Heuristiken zur Erkennung von Betrug. Dies entspricht auch der Auffassung von Sicherheitsforscher:innen, dass Verbraucher:innen an sich ein gut entwickeltes Sensorium für Unstimmigkeiten haben.[21] Allerdings sind Systeme, Prozesse und die Argumentationen der Anbieter in Schadensfällen aktuell eher darauf ausgelegt, die geschädigten Verbraucher:innen als Problemfaktor zu sehen. Das bedeutet, dass Systeme so aufgebaut sind, dass sie zwar technisch sicher sein mögen, aber unverständlich sind (siehe voriges Kapitel), Fehler nicht verziehen werden und die an sich vorhandene intuitive Fähigkeit zum richtigen Handeln auch bei veränderten Angriffsszenarien nicht produktiv eingebunden wird. Dies kann zum Beispiel durch den Einbau von Redundanzen erfolgen, sodass ein einziger falscher Klick nicht bereits zur kompletten Übernahme eines Kontos durch Betrüger:innen führen kann. „Compliance“, so die beiden Sicherheitsforscherinnen Verena Zimmermann und Karen Renaud, „becomes the mantra. Yet compliance only enhances security if the attackers do not innovate and change strategies, and only if the system is decomposable. Both of these assumptions, however, are unrealistic.”[22]

5. FOLGEN BEI OPFERN EINES BETRUGS

Personen, die auf die betrügerischen Fallkonstellationen eingegangen wären, wurden am Ende darüber aufgeklärt und befragt, ob und welche Konsequenzen sie daraus zögen. Die große Mehrheit (72 Prozent) dieser Befragtengruppe gab an, künftig sehr viel aufmerksamer zu sein. Für insgesamt 43 Prozent der Befragten bedeutete dies aber

[21] So erklärt Kristin Weber, Professorin für IT-Management und IT-Organisation: „Menschen sind in der Lage, Dinge zu erkennen, die die IT heute noch nicht erkennen kann. Und häufig reagieren wir intuitiv richtig.“ (Weber, Kristin; Hauck, Mirjam: „Es reicht, wenn ein paar klicken“, in: Süddeutsche Zeitung, 20.03.2024)

[22] Zimmermann, Verena; Renaud, Karen: Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset, in: International Journal of Human-Computer Studies, 2019, S. 169–187, S. 174.

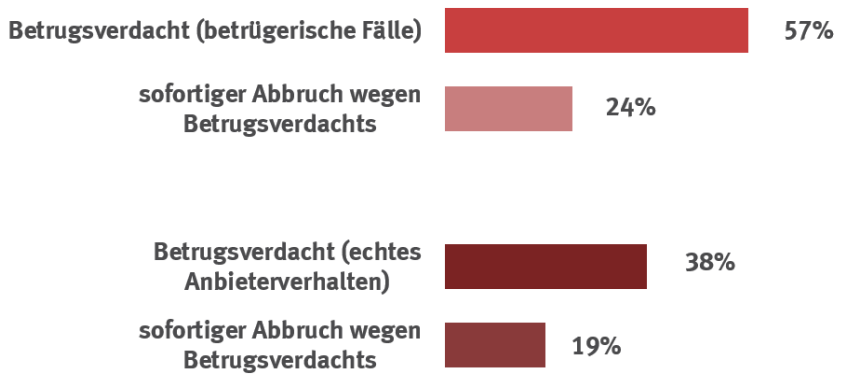
gravierendere Einschnitte in ihrem Verhalten: 19 Prozent gaben an, sie würden künftig kein Onlinebanking mehr machen. 13 Prozent dieser Befragtengruppe würden nichts mehr im Internet bezahlen. Und 29 Prozent erklärten, ihr digitales Leben stärker einschränken zu wollen.[23]

6. ECHTES ANBIETERVERHALTEN

In Gegenüberstellung zu den betrügerischen Fallkonstellationen wurden die Befragten auch mit Szenarien konfrontiert, die von echten Anbietern stammten. Mit 33 Prozent lehnten es fast identisch viele Teilnehmer:innen wie bei den betrügerischen Fällen grundsätzlich ab, auf das Anliegen einzugehen oder brachen den entsprechenden Vorgang ab.[24] Von dieser Befragtengruppe begründeten 59 Prozent ihre Weigerung explizit mit einem Betrugsverdacht.[25] Zusätzlich äußerten weitere 13 Prozent der Befragten ebenfalls einen Betrugsverdacht, wollten sich aber zunächst mit einer dritten Person besprechen. 2 Prozent der Befragten waren zwar bereit, auf das Anliegen einzugehen, fanden das Vorgehen aber verdächtig.

Insgesamt äußerten somit über die zehn getesteten echten Fallkonstellationen 38 Prozent der Befragten den Verdacht, dass es sich um Betrug handeln könnte. 19 Prozent lehnten es wegen dieses Verdachts direkt ab, auf das Anliegen einzugehen bzw. brachen den entsprechenden Vorgang ab.[26]

Grafik 4: Anteil der Fälle mit Äußerung eines Betrugsverdachts und sofortige Abbrüche:



Im Hinblick auf die Prozessverläufe, die im normalen Bankgeschäft zwingend abzuwickeln sind, fällt auf, dass eine ganze Reihe an Kommentaren der Teilnehmer:innen der Befragung deren Komplexität und Unverständlichkeit betonte. So bewerteten Befragte die dargestellten echten Abläufe mit „umständlich“, „kompliziert“, „verwirrend“, „nicht einfach“, „verstehe nicht, warum es nicht klappen soll“, „ist ziemlich fremd“, „komische Reihenfolge“, „nicht ein Vorgehen, das mich in Sicherheit wiegt“, „ich bin verunsichert“,

[23] Basis: Befragte, die auf eine betrügerische Fallkonstellation eingegangen wären. Mehrfachnennungen möglich.

[24] Ergebnisse im Detail: Für die Fallkonstellationen B-J: 11 Prozent erledigen Anliegen nicht gleich, aber später, 27 Prozent erledigen es sofort, 32 Prozent gehen nicht auf das Anliegen ein, 24 Prozent besprechen sich zunächst mit dritter Person, 7 Prozent wählen ein sonstiges Vorgehen. Für Fallkonstellation A: 53 von 96 geben das Passwort ein, 43 von 96 geben es nicht ein. Als grundsätzliche Ablehnung, auf das Anliegen einzugehen, wurden die Stimmen gewertet, die nicht auf das Anliegen eingingen (B-J) oder die das Passwort nicht eingaben (A). Basis: 1.035 Befragte

[25] Basis: Befragte, die das echte Anbieterverhalten ablehnten

[26] Basis: 1.035 Befragte. Kumulierte Werte über alle zehn nicht betrügerischen Fallkonstellationen

„warum einfach, wenn kompliziert auch geht!“, „ich bin überfordert“. Wenn Prozesse so gestaltet sind, dass Nutzer:innen deren Struktur und Sinn nicht verstehen können, ist es ihnen auch kaum möglich, auffällige Abweichungen im Falle eines Betrugs zu erkennen. Das gelernte Verhalten besteht dann einfach darin, dass das Geforderte erledigt werden muss, egal wie unverständlich es sein mag. Darüber hinaus zeigen die Beispiele mit Fehlermeldung bzw. einer überflüssigen, nicht responsiven TAN-Eingabe (Fallkonstellationen J und A), dass Verbraucher:innen aufgrund einer defizitären Produktgestaltung teilweise gezwungen sind, einen gewissen Grad an Auffälligkeiten zu tolerieren, wenn sie sich aus der Teilhabe am Zahlungsverkehr nicht aussperren wollen.

FAZIT

Im Ergebnis war festzustellen, dass betrügerisches Anbieterverhalten in den geprüften Fallkonstellationen von den Befragten zwar mehrheitlich als Betrug erkannt wurde (57 Prozent). Tatsächlich verhielten sich allerdings auch echte Anbieter in einer Weise, die die Befragten in 38 Prozent der geprüften Fälle Betrug vermuten ließen. Durch die hohen Ähnlichkeiten zwischen betrügerischem und nicht betrügerischem Verhalten, werden aus Sicht des vzbv die Fähigkeiten der Verbraucher:innen zur Erkennung von Betrug nicht ausreichend unterstützt.[27]

Außerdem waren die Warnmeldungen, die Anbieter versendeten, um Kund:innen beispielsweise auf eine betrügerische Einrichtung eines Authentisierungsinstruments hinzuweisen, im Kontext kaum hilfreich. Sie wurden unter anderem als schlecht verständlich beschrieben und waren nicht standardisiert, sodass Befragte nicht erkennen konnten, welcher Vorgang damit angezeigt wird, und die Mails mitunter fehlinterpretierten. Die Warnmeldungen trugen also unter Umständen gerade dazu bei, dass die Befragten sich in Sicherheit wogen, obwohl Betrüger:innen gerade ggf. freier Zugriff auf das Konto gewährt wurde. Derartige Systeme sind nicht resilient konstruiert[28] und scheinen darüber hinaus davon auszugehen, dass Verbraucher:innen sich vollständig mit Prozessen und Termini des Zahlungsverkehrs auskennen. Zusätzlich setzen sie hohe Anforderungsniveaus: Selbst für die Ausführung einer Überweisung muss beispielsweise zuvor die Internetseite eines Anbieters für aktuelle Sicherheitswarnungen konsultiert werden, um auszuschließen, dass im Betrugsfall nicht der Vorwurf der groben Fahrlässigkeit erhoben wird. Das Angebot von immer mehr Informationen zum Themenfeld auf Anbieterseite oder bei anderen relevanten Akteuren[29] verlagert die vermeintlichen Pflichten für die sichere Teilhabe an Bankgeschäften zunehmend einseitig auf die Verbraucher:innen. Hierbei besteht aus Sicht des vzbv die Gefahr, dass Verbraucher:innen sich aus Angst aus dem digitalen Zahlungsverkehr zurückziehen. 43 Prozent der Befragten, die auf eine betrügerische Fallkonstellation eingegangen wären, haben derartige Konsequenzen angekündigt, wenn sie Opfer eines solchen Betrugs würden.

[27] Siehe hierzu Zimmermann/Renaud [Fn. 22].

[28] „Resilience is understood as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions“ (Hollnagel, Erik; Fujita, Yushi: The Fukushima Disaster – Systemic Failures as the Lack of Resilience, in: Nuclear Engineering and Technology, H. 1, 2013, S. 13).

[29] Vgl. beispielsweise https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html, 22.03.2024; https://www.bleib-virenfrei.de/it-sicherheit/phishing-rufnummern/, 22.03.2024; https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing/, 22.03.2024.

Neben den überprüften Fällen bestehen in einem Graubereich zusätzlich die Konstellationen, bei denen nicht Verbraucher:innen die Angegriffenen sind, sondern die Anbieter selbst. Hierzu werden keine Daten veröffentlicht, aber Betrüger:innen nutzen immer mehr Ressourcen, um die Unternehmen anzugreifen. 2023 wurden täglich 70 neue Schwachstellen in Softwareprodukten entdeckt.[30] Verbraucher:innen können dabei leider nicht immer davon ausgehen, dass die Unternehmen Sicherheitsvorfälle korrekt kommunizieren.[31] Und selbst wenn Unternehmen nicht direkt selbst angegriffen werden, scheint die Behauptung von Anbietern, ihre Systeme seien sicher, angesichts der vielen Einfallstore für menschliche Fehler auf Entwickler- und Unternehmensseite[32] naiv. Die technische Sicherheit von Bankanwendungen wie Authentisierungsinstrumenten kann derzeit nicht öffentlich überprüft werden, beispielsweise durch Zugang zu einer Testumgebung und Bereitstellung relevanter Informationen. Anbietern ist es daher möglich, ihre Technik als unüberwindbar sicher darzustellen und den Betrugsopfern Schadensersatz zu verweigern. Es ist dann weiterhin ohne Vorlage von eindeutigen Beweisen möglich zu behaupten, Verbraucher:innen hätten betrügerische Transaktionen selbst autorisiert und könnten nur grob fahrlässig auf Social Engineering eingegangen sein.

Insgesamt lässt sich konstatieren, dass

1. betrügerische Angriffe keinesfalls leicht und zuverlässig erkannt werden können, dass
2. echtes Anbieterverhalten mitunter von betrügerischem Verhalten nicht leicht zu unterscheiden ist, dass
3. Warnmeldungen von Anbietern ihren Zweck nicht immer gut erfüllen, dass
4. viertens ein strukturelles Informationsdefizit für Verbraucher:innen im Hinblick auf mögliche Sicherheitsvorfälle besteht und ihnen gleichzeitig hohe Informationspflichten als Holschuld auferlegt werden.

Im Hinblick auf die eingangs erwähnte Haftungsfrage kann im Ergebnis nicht bestätigt werden, dass Verbraucher:innen, die Opfer eines Betrugs (z. B. einer Phishing-Mail) werden, allein durch das Eingehen auf das betrügerische Handeln bereits grob fahrlässig handeln würden. Für sich allein kann dies aufgrund der Erkenntnisse der vorliegenden Untersuchung kein Beleg für eine außergewöhnliche Nachlässigkeit sein.

[30] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2023. S. 11f.

[31] Siehe beispielsweise Deutsche Bank AG: BaFin setzt Geldbuße fest, 2024, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_2024_03_18_Deutsche_Bank_AG.html?nn=19645206&cms_expanded=true, 19.03.2024.

[32] Siehe hierzu Renaud, Karen: Human-Centred Cyber Secure Software Engineering, in: Zeitschrift für Arbeitswissenschaft, H. 1, 2023, S. 45–55. Darüber hinaus und hierbei noch gänzlich unbeachtet sind absichtlich durchgeführte Angriffe von Mitarbeiter:innen aus den Unternehmen selbst, siehe hierzu Weber, Kristin; Schütz, Andreas E; Fertig, Tobias: Insider Threats – Der Feind in den eigenen Reihen, in: HMD Praxis der Wirtschaftsinformatik, H. 3, 2020, S. 613–627.