BioCatch

Betrugstrends im Online-Banking 2024 in Deutschland

Bericht von BioCatch über die aktuelle Bedrohungslage im Onlinebereich in Deutschland.

April 2024

Über diesen Bericht

Für die Erstellung dieses Berichts führte das Expertenteam von BioCatch unter der Leitung seines weltweiten Beraterteams und seiner Bedrohungsanalysten Recherchen zur Bedrohungslage in Deutschland durch.

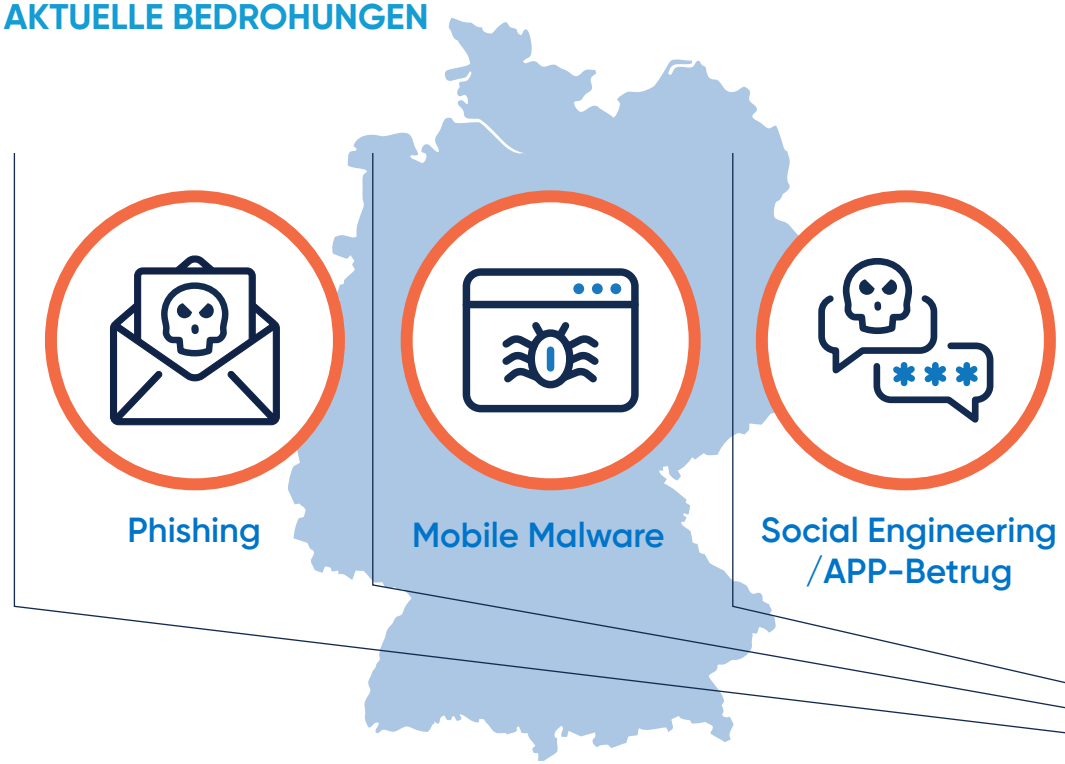
Dieser Bericht bietet einen umfassenden Überblick über die aktuelle Bedrohungslage und die Betrugstrends im Bankbereich in Deutschland. Wir fokussieren uns insbesondere auf das ständig wachsende Phishing-Problem und seine Auswirkungen auf deutsche Banken.

Dieser Bericht ist in folgende Abschnitte unterteilt:

- Bedrohungslage in Deutschland
- Anatomie eines Phishing-Angriffs
- Deep Dive: Phishing-Angriffe
- Analyse der Finanzlandschaft in Deutschland

Bedrohungslage in Deutschland

AKTUELLE BEDROHUNGEN



Beispiele für Phishing:

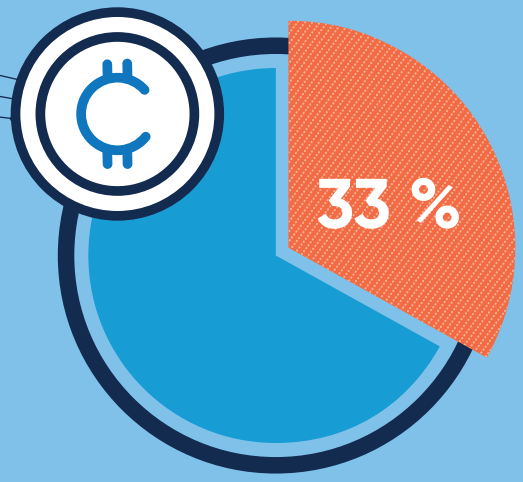
- Aktualisierungen von Bankdaten
- Kontosicherheit
- Paketzustellung
- Steuerbescheide

Beispiele für Social-Engineering-Betrug:

- Ausgeben als Bankmitarbeiter
- Anlagen und Kryptowährung
- Einkauf/Online-Shopping
- Romantik/Online-Dating
- Gefälschte Stellenausschreibungen

1 von 3

Zwar haben 84 % der Deutschen bereits von Kryptowährung gehört, dennoch hat nur ein Drittel der Befragten ein vollumfängliches Verständnis für die Funktionsweise von Kryptowährungen, so dass mehr als 30 % der deutschen Bevölkerung anfällig für Krypto-Betrug sind.[1]



1 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2311_Digitalisierung.html

Anatomie eines Phishing-Angriffs

1. Der Betrüger erhält Benutzerdaten, wahrscheinlich aus dem Darknet.
2. Der Betrüger versendet E-Mails, die mit rechtmäßig wirkendem Branding den Eindruck erwecken, dass sie von einer Bank oder Behörde stammen.
3. Das Opfer klickt auf Links in der E-Mail.
4. Das Opfer landet auf einer gefälschten Website (Phishing-Seite), wo es zur Eingabe von personenbezogenen Daten oder Zugangsdaten aufgefordert wird.
5. Das Opfer gibt die Daten ein.
6. Der Betrüger erhält die Informationen von der Phishing-Seite und stiehlt das Geld des Opfers.

BioCatch

DEEP DIVE:

Phishing-Angriffe

Was ist Phishing?

Phishing ist eine Form des Social Engineering. Dabei werden schriftliche Nachrichten – in der Regel E-Mails – versendet, die scheinbar von seriösen Quellen stammen, um die Zielpersonen zur Preisgabe personenbezogener Daten zu zwingen.

Andere Formen des Phishing sind unter anderem Smishing (mittels SMS) oder Vishing, Kurzform für „Voice Phishing" (mittels eines Telefonanrufs).

Was ist ein Beispiel?

Die Opfer erhalten eine E-Mail, die vorgibt, von einer Bank, einer Behörde oder einem Online-Händler zu stammen. Die Nachricht enthält einen Link sowie Text, der die Nutzer auffordert, auf den genannten Link zu klicken, um für ihr Konto einige Aktionen durchzuführen. So werden die Nutzer beispielsweise aufgefordert, ein Sicherheitsupdate durchzuführen, um das Online-Banking weiterhin nutzen zu können, ihre Kontodaten zu aktualisieren, um die AML-Vorschriften einzuhalten, oder sie werden darüber informiert, dass zur Vermeidung einer Geldstrafe eine dringende Steuerzahlung erforderlich ist.

Was geschieht als Nächstes?

Wenn die Empfänger an die Rechtmäßigkeit der E-Mail glauben, klicken sie auf den Link und gelangen auf eine Phishing-Website, die der echten Website, die sie imitiert, sehr ähnlich ist. Auf dieser Website wird die Eingabe personenbezogener Daten verlangt und sobald die Nutzer diese Daten eingeben, sind die Betrüger im Besitz ihrer Zugangsdaten und können online auf ihr Bankkonto zugreifen.

DEEP DIVE:

Phishing-Angriffe

Wie gehen die Betrüger vor?

Sobald die Betrüger die Zugangsdaten der Nutzer haben, können sie auf die Bankkonten der Opfer zugreifen und nach Belieben Transaktionen durchführen, oft ohne Einschränkungen. Hauptziel der Betrüger ist die Veranlassung von Zahlungen, aber es gibt auch Betrüger, die Kredite aufnehmen, um zusätzliche Mittel zu beschaffen, die sie sich auszahlen lassen können.

Manche Betrüger verwenden sogar die erhaltenen Zugangsdaten in Echtzeit. Das kommt vor allem dann vor, wenn Zweifaktor-Authentifizierung verlangt wird. Die betrügerischen Akteure verwenden die Phishing-Website, um von den Opfern diese zusätzlichen Informationen zu erlangen, wie beispielsweise Einmalpasswörter (OTPs). Auch dies erfolgt in Echtzeit, unter dem Vorwand, dass die Codes zur „Ausführung des Prozesses" erforderlich seien.

Was sollten Sie als Opfer eines Phishing-Angriffs tun?

Vorsorge ist besser als Nachsorge. Auch wenn es unvermeidlich ist, dass Sie irgendwann Phishing-E-Mails erhalten, können Sie durch Ihre Reaktionsart vermeiden, Opfer eines Betrugs zu werden.

Viele Behörden und Organisationen sind sich bewusst, dass Aufklärung die beste Waffe ist, und setzen sich dafür ein, das Bewusstsein rund um diese betrügerischen Kampagnen zu erweitern.

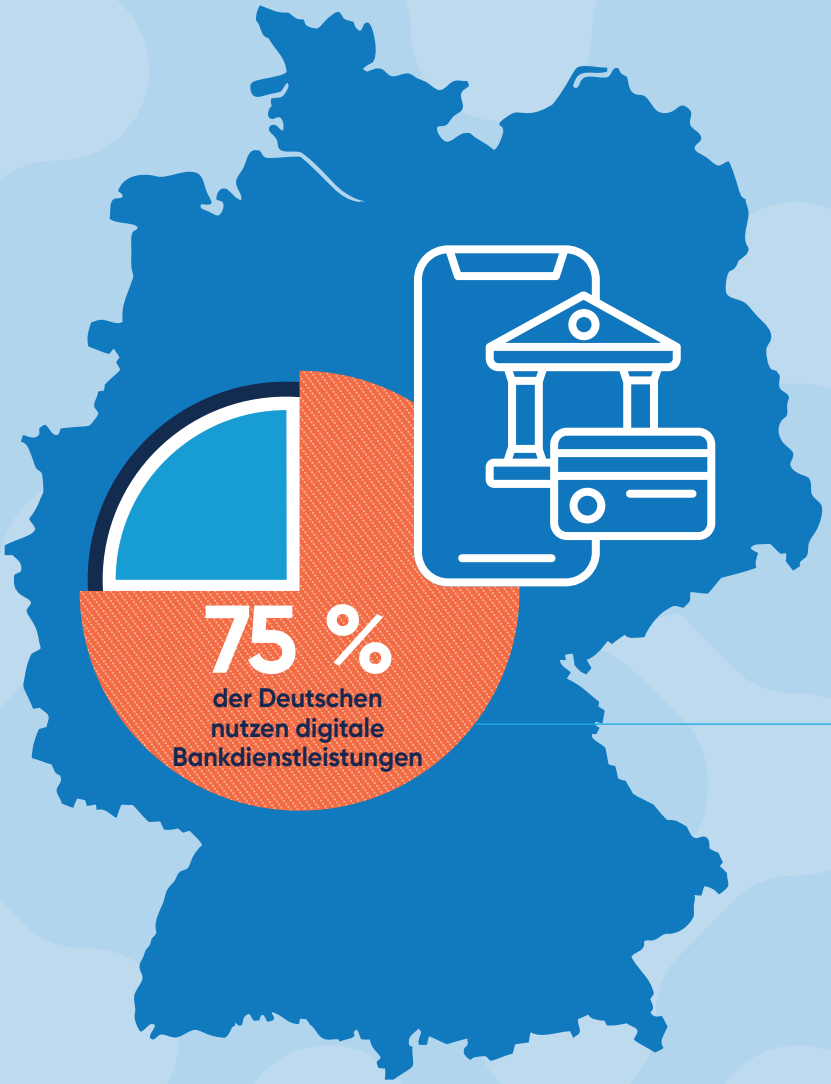
Die deutsche Zollbehörde, die für Zölle, Steuern und die Verfolgung von Geldwäsche zuständig ist, hat selbst einen Ratgeber[1] für die deutschen Bürger herausgegeben, der beschreibt, wie sie sich schützen können. Ebenso gibt das BSI (Bundesamt für Sicherheit in der Informationstechnik) ausführliche Informationen über Phishing-Angriffe heraus, einschließlich einer Webseite, die Beispiele für Phishing-E-Mails aufzeigt[2].

Wann immer Sie eine verdächtige E-Mail erhalten, ist es am besten, ihre Rechtmäßigkeit überprüfen. Dazu können Sie die unten verlinkten Ressourcen heranziehen oder sich direkt an die Bank oder das Unternehmen wenden.

SCHON GEWUSST?

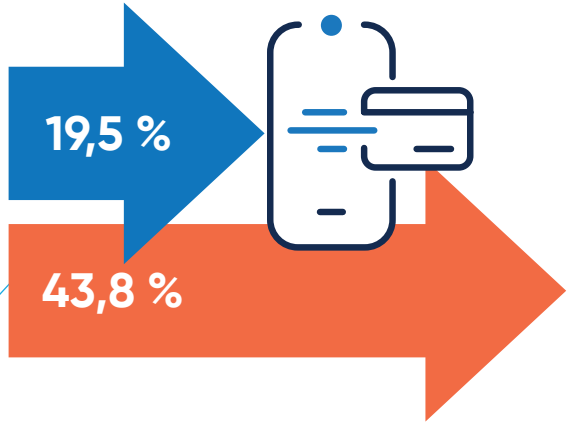
Nur 2 % der Verbraucher gaben zu, nach dem Erhalt von Betrugsnachrichten gegen ihren Willen personenbezogene Daten (Passwörter, Kartendaten usw.) preisgegeben zu haben.[3]

1. https://www.zoll.de/Private-individuals/Postal_consignments_internet_order/Maliciou-%20phishing-emails-fraudulent-cus-toms-tax-assessments/maliciou-%20phishing-emails-fraudulent-customs-tax-assessments_node.html
2. https://www.bsi.bund.de/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/akttuelle-beispiele-fuer-phishing.html
3. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2311_Digitalisierung.html



Analyse der Finanzlandschaft in Deutschland

Deutschland ist zwar die größte Volkswirtschaft in der EU, hinkt bei der Digitalisierung und Nutzung mobiler Zahlungen jedoch hinter anderen europäischen Territorien wie beispielsweise Großbritannien hinterher. Derzeit nutzen 75 % der Deutschen Online-Banking-Dienste, um einfache Aufgaben wie die Überprüfung des Kontostands oder die Online-Bezahlung von Rechnungen zu erledigen, aber weniger als 40 % nutzen moderne digitale Bankdienstleistungen wie Online-Anträge für Konten oder Karten (39 %), Konto-Aggregatoren (30 %) oder digitale Geldbörsen (27 %).[1]



Die jährliche Zunahme an mobilen Zahlungen beläuft sich auf 43,8 % – mehr als das Doppelte als die 19,5 % in Großbritannien.

Dies scheint sich jedoch zu ändern, denn wir sehen ein jährliches Wachstum von 43,8 % bei der Akzeptanz mobiler Zahlungen – mehr als das Doppelte als die 19,5 % in Großbritannien[2] Mit der zunehmenden Akzeptanz von digitalen Bankdienstleistungen steigt auch das Risiko für die Verbraucher.

Das Risiko wird zudem noch durch die wachsende Zahl an Neobanken in Deutschland erhöht, die ein rein digitales Angebot haben und allmählich zu den etablierten Bankengruppen aufschließen.[3]

1. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2311_Digitalisierung.html
2. https://www.trade.gov/market-intelligence/germany-financial-technology-fintech
3. https://fintech.global/2023/08/28/incumbent-banks-dominate-mobile-banking-in-germany/

AKTUELLE SITUATION:

Betrügerische Angriffe

Die PSD2-Verordnung zwang Deutschland genau wie alle anderen EU-Länder dazu, strenge Kontrollen zur Kundenauthentifizierung einzuführen, allerdings unterscheidet sich Deutschland von vielen anderen EU-Ländern durch die Art der am häufigsten auftretenden Angriffe. Während sich die Betrüger in vielen anderen europäischen Ländern auf Social-Engineering-Scam fokussieren – vor allem in den Niederlanden, Spanien und den nordischen Ländern – sind die Betrugsmaschen in Deutschland noch nicht so ausgefeilt. Das Land hat jedoch immer noch ein Problem mit Phishing, das häufig in Form von Echtzeit- oder Man-in-the-Middle-Angriffen erfolgt. Dabei versuchen die Betrüger, Autorisierungscodes zu erhalten – seien es TAN-Codes, In-App-Autorisierungscodes oder sogar vom Opfer selbst eingegebene TAN- oder In-App-Codes.

Es ist also nicht so, als ob es in Deutschland keinen Betrug geben würde. Tatsächlich sehen sich die Banken in Deutschland mit vielen Betrugsmaschen konfrontiert, die auch anderswo in Europa und der Welt angewendet werden. Die beiden wichtigsten Betrugsmaschen in Deutschland sind Identitätsbetrug (wenn sich Betrüger als Vertreter von Banken oder anderen offiziellen Stellen ausgeben und eine dringende Geldüberweisung anfordern) und Investment Scams. Letzteres kommt wahrscheinlich häufiger vor, da die Menschen lieber sparen als Geld ausgeben (ein Muster, das wir auch in der Schweiz beobachten). Infolge sind Fake-Shops, wie sie in anderen Teilen Europas weitverbreitet sind, in Deutschland ein kleineres Problem.

Deutschland hat glücklicherweise eine der besten Finanzmarktregulierungen der Welt und die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) gibt Warnungen zu digitalen Betrugsrisiken heraus. Sie überwacht auch Unternehmen, die vorgeben, eine BaFin-Zulassung zu haben, und sind federführend bei der Identifizierung von Investment Scams.

In Deutschland gehen Investment Scams häufig von deutschen Muttersprachlern aus, die von Osteuropa aus agieren (im Gegensatz zum englischsprachigen Raum, wo die Angriffe meist aus Asien stammen). Dadurch wirkt diese Betrugsmasche, die deutsche Banken und ihre Kunden ins Visier nimmt, besonders glaubwürdig, so dass es für die Opfer schwieriger wird, diese Angriffe als solche zu erkennen.

Unsere Recherchen zeigen, dass Phishing-Kampagnen der Ausgangspunkt für diese Betrugsversuche sind. Somit bietet sich die Chance, sie bereits gleich zu Beginn zu stoppen. Andere Methoden der Kontaktaufnahme sind gefälschte Werbeanzeigen, wobei manchmal echte Handels- und Anlageplattformen nachgeahmt werden, um die Opfer dazu zu veranlassen, eine Anfrage zu stellen und den Kontakt mit den Betrügern aufzunehmen. Dank der koordinierten internationalen Bemühungen von Organisationen wie Europol haben sich die deutschen Strafverfolgungsbehörden glücklicherweise als sehr effektiv beim Zerschlagen einiger dieser Ringe erwiesen[1].

Deutschland unterscheidet sich von vielen anderen EU-Ländern durch die Art der am häufigsten auftretenden Angriffe. Die beiden wichtigsten Betrugsmaschen, unter denen das Land zu leiden hat, sind Identitätsbetrug und Investment Scam.

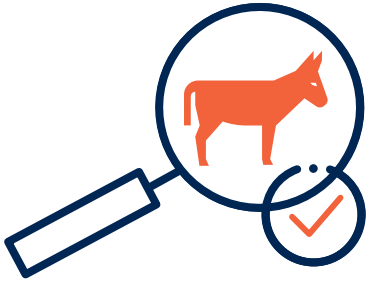
1. https://www.occrp.org/en/daily/18200-police-across-europe-target-more-boiler-room-scams

AKTUELLE SITUATION:

Mules und AML

Deutsche Banken standen in den letzten Jahren aufgrund ihrer Versäumnisse bei der Geldwäschebekämpfung (AML) im Rampenlicht. Die daraus resultierenden Bußgelder führten zu Verbesserungen bei den Kontrollen, die zur Identifizierung von Hochrisikokonten eingeführt wurden. In anderen Ländern war die Situation ähnlich: Große Bußgelder veranlassten die Banken, viel Geld für die Implementierung strengerer Kontrollen in die Hand zu nehmen.

Leider ist als einer der Nebeneffekte seit Neuestem eine niedrige Risikotoleranz zu beobachten, was für die Endnutzer mehr Reibungsverluste bedeutet. Es wurde mehrfach von Privatkonten berichtet, die wegen des Verdachts auf Geldwäsche eingefroren oder sogar gesperrt wurden. Aufgrund der manuellen Prozesse bei AML-Untersuchungen haben die Kontoinhaber dann oft wochenlang keinen Zugang zu ihrem Geld oder sogar zur digitalen Bankensphäre. In einer zunehmend digitalen Welt kann dies für Kunden verheerende Folgen haben. Bisher waren die Banken aufgrund des Geldwäschegesetzes (§ 48) vor jeglicher Verantwortung gegenüber den Kunden geschützt, aber die Betroffenen wehren sich nun mit dem Argument[1], dass die Banken nicht alle ihnen zur Verfügung stehenden Informationen nutzen. Weil AML-System meist regelbasierte Systeme mit einer relativ niedrigen Wirksamkeit sind, sind sie anfällig für hohe Fehlalarm-Quoten, was unnötige Reibungsverluste und Konsequenzen für die Kunden nach sich zieht. Durch einige Gerichtsverfahren werden die Banken nun daran erinnert, dass ihre Haftungsbefreiung kein Freibrief für ungerechtfertigte Sperrungen ist. Das lenkt den Fokus wieder auf die Banken zurück, die sicherstellen müssen, dass ihre Kontrollen sowohl wirksam als auch robust sind.



Weil AML-System meist regelbasierte Systeme mit einer relativ niedrigen Wirksamkeit sind, sind sie anfällig für hohe Fehlalarm-Quoten, was unnötige Reibungsverluste und Konsequenzen für die Kunden nach sich zieht.

1. https://www.handelsblatt.com/finanzen/steuern-recht/recht/geldwaescheverdacht-gerichte-sehen-banken-in-der-haftung-fuer-falsche-kontosperrungen/100014693.html?utm_source=sf&utm_medium=nl&utm_campaign=hb-financebriefing&utm_content=21022024&key=0037S00000UoLSqQAN

AKTUELLE SITUATION:

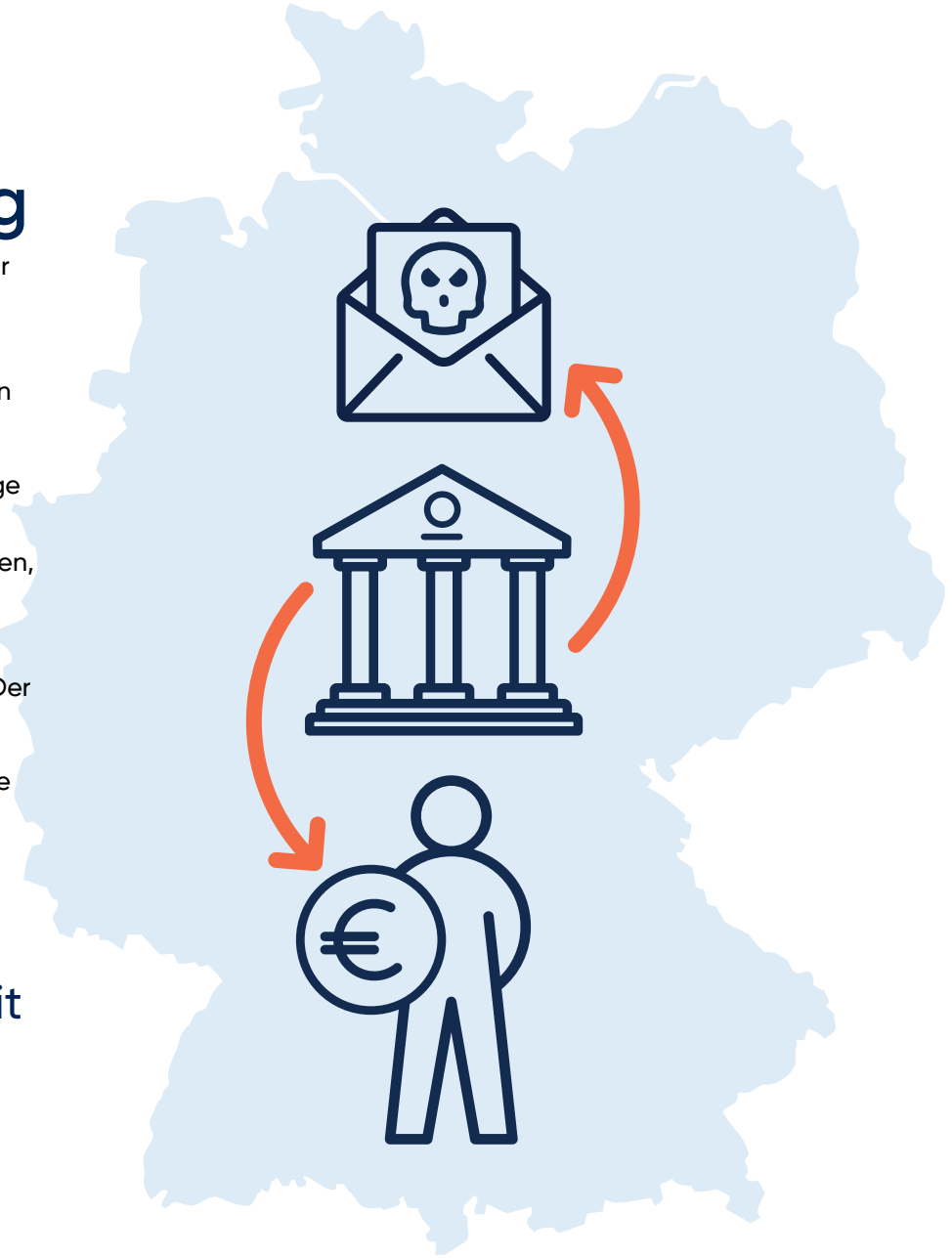
Betrug und Erstattung

Da die PSD2-Verordnung die Banken dazu verpflichtet, nur nicht autorisierte Betrugsfälle (z. B. Phishing) zu erstatten, und der zusätzliche Vorbehalt der groben Fahrlässigkeit zu Unklarheiten darüber führt, wann eine Erstattung zu leisten ist (Banken müssen Opfer nicht entschädigen, wenn das Opfer fahrlässig gehandelt hat, d. h. indem es starke Authentifizierungscodes preisgibt), gibt es in Deutschland im Vergleich zu anderen europäischen Ländern nur niedrige Erstattungsquoten.

Aktuell gibt es keine regulatorische Verpflichtung für Banken, autorisierte Zahlungen zu erstatten (d. h. Betrug). Das hat einen Graubereich zur Folge, der sich von Bank zu Bank unterscheidet und oft von den individuellen Umständen abhängt. Mit PSD3 wird sich dies voraussichtlich ändern. Der im letzten Jahr ursprünglich vorgelegte Vorschlag enthält Richtlinien zu Erstattungen in Bezug auf verschiedene Betrugsmaschen, insbesondere Identitätsbetrug, wenn die Identität der Bank imitiert wurde.

Das veranlasst deutsche Banken, bessere Kontrollen einzuführen, um angesichts der Einführung von PSD3 Betrugsfälle zu verhindern.

Deutschland hat im Vergleich mit anderen europäischen Ländern niedrige Erstattungsquoten.



"Viele Banken haben ihren Schwerpunkt dahingehend verlagert, dass sie nun eine ganzheitliche Sicht auf den Kunden-Lebenszyklus erhalten wollen, um das Nutzerverhalten besser zu verstehen."

Iain Swaine, Director of Global Advisory für EMEA bei BioCatch

DIE ZUKUNFT:

Weitere Entwicklungen

Europaweit beobachten wir eine signifikante Zunahme an autorisiertem Zahlungsbetrug. Es ist wahrscheinlich, dass in den nächsten Jahren dieser Trend auch in Deutschland Einzug halten wird.

Die rasche Entwicklung der generativen KI wird voraussichtlich zu einem Anstieg der Angriffe auf Deutsche führen, da sie die Sprachbarriere beseitigt und den Betrügern eine größere Auswahl an Zielen bietet, ganz zu schweigen von der Möglichkeit, Angriffe in größerem Umfang zu industrialisieren. Tatsächlich erleben wir bereits Vorgehensweisen, die Deep-Fake-Technologie verwenden – ob Audio oder Video – um noch verlockendere Betrugsmaschen zu ersinnen und die Taktiken der Betrüger zu verfeinern.

In Großbritannien, wo die Regulierungsbehörde für den Zahlungsverkehr (Payment System Regulator, PSR) bahnbrechende Erstattungsvorschriften erlassen hat (hier wird die Haftung zwischen der absendenden und der empfangenden Bank aufgeteilt), haben die Banken begonnen, die Art und Weise der Betrugserkennung zu revolutionieren. Dies hat zusammen mit einem verstärkten Fokus auf AML-Kontrollen durch Regulierungsbehörden dazu geführt, das viele Banken den Schwerpunkt ihrer Untersuchungen verlagern. Wir erleben, dass Banken eine ganzheitliche Sicht auf den Kunden-Lebenszyklus anstreben, um das Nutzerverhalten besser zu verstehen, damit sie AML-Bedenken ausräumen sowie mögliche Mule-Konten identifizieren können, die das Risiko für die Bank erhöhen könnten.

ÜBER BIOCATCH

BioCatch steht an vorderster Front der Erkennung von digitalem Betrug und leistet Pionierarbeit beim Einsatz von verhaltensbiometrischer Intelligenz basierend auf fortschrittlicher Kognitionswissenschaft und maschinellem Lernen. BioCatch analysiert Tausende Interaktionen von Anwendern, um eine Onlinebanking-Umgebung zu schaffen, in der Identität, Vertrauen und Benutzerfreundlichkeit sich nicht ausschließen. Heute setzen mehr als 30 der 100 größten Banken sowie mehr als 180 der 500 größten Banken weltweit auf BioCatch Connect™, um Betrug zu bekämpfen, die digitale Transformation voranzubringen und Kundenbeziehungen zu stärken. Das Client Innovation Board von BioCatch, eine von der Finanzbranche angeführte Initiative, der American Express, Barclays, Citi Ventures, HSBC und National Australia Bank angehören, arbeitet zusammen, um kreative und innovative Lösungen zu entwickeln, die die Kundenbeziehungen zur Betrugsprävention nutzen. Mit mehr als einem Jahrzehnt Erfahrung in der Datenanalyse, über 90 angemeldeten Patenten und konkurrenzloser Expertise leistet BioCatch weiter Pionierarbeit, um künftigen Herausforderungen zu begegnen. Weitere Informationen finden Sie unter www.biocatch.com.

BioCatch