Betrug entdecken

Die gängigsten Betrugsmuster erklärt

Zürcher Kantonalbank

Inhalt

Betrug entdecken

Betrugsmaschen unter der Lupe

In einer Welt, die zunehmend vernetzt ist, sind Betrugsdelikte eine ernsthafte und tägliche Herausforderung. Es handelt sich sowohl um raffinierte Internetbetrügereien wie auch traditionelle Methoden, die durch moderne Technologien professionalisiert werden. Daher ist es entscheidend, die verschiedenen Arten von Betrug zu erkennen und zu verstehen – denn es kann uns alle treffen, unabhängig von Alter, Geschlecht oder Standort. Von Internetbetrug bis hin zu Telefonbetrug, Kreditkartenbetrug und Identitätsdiebstahl, der Aufbau ist immer ähnlich:

1) Das unwiderstehliche Angebot
2) Die absolut nötige Investition oder Zahlung
3) Die Enttäuschung

Diese Broschüre beleuchtet die verschiedenen Facetten der häufigsten «Scams» und gibt Ihnen wertvolle Tipps, wie Sie sich schützen können. Die folgenden Szenarien zeigen den möglichen Ablauf eines «Scams» auf.

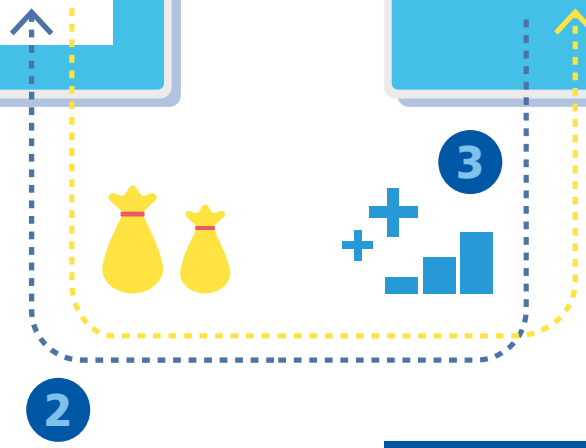
Das schnelle Geld

Investment Scam

Betrügerinnen und Betrüger werben online mit lukrativen Investitionsmöglichkeiten, die schnell viel Gewinn generieren.
Oft werden in diesen Werbungen berühmte Persönlichkeiten verwendet, die damit ein Vermögen gemacht haben.

Ausweisdokumente verlangen
Gehen Sie auf die Werbung ein, nehmen die betrügenden Personen schnell Kontakt auf und bieten ihre Unterstützung an, auch bei der Kontoeröffnung. Dazu verlangen sie entsprechende Unterlagen (zum Beispiel Pass oder ID). Zudem werden Sie aufgefordert, eine erste Zahlung zu erfassen.

Gefälschte Gewinne vorgaukeln
Die Betrügerinnen und Betrüger leiten Sie bei ihren regelmässigen telefonischen Kontakten auf gefälschte Dashboards, um angebliche Gewinne auszuweisen. So werden Sie dazu gebracht, weiteres Geld zu investieren.



Immer mehr Geld anfordern
Sie werden immer wieder dazu gebracht, mehr Geld zu investieren, indem man konsequent und hartnäckig auf Sie einredet. Dabei können Ihnen die Betrügerinnen und Betrüger kleinere Beträge auszahlen, um Vertrauen zu gewinnen. Sobald nichts mehr zu holen ist, brechen die Betrügerinnen und Betrüger den Kontakt ab. Das Geld ist längst auf andere Konten weitergeleitet worden und Sie verlieren den vollständigen Investitionsbetrag.

- **Gehen Sie nicht auf Online-Werbung ein, die schnelles Geld verspricht.**
- **Schicken Sie Ihre persönlichen Dokumente (oder Kopien davon) niemals an unbekannte Dritte.**
- **Investieren Sie kein Geld in Ihnen unbekannte Firmen oder Personen.**

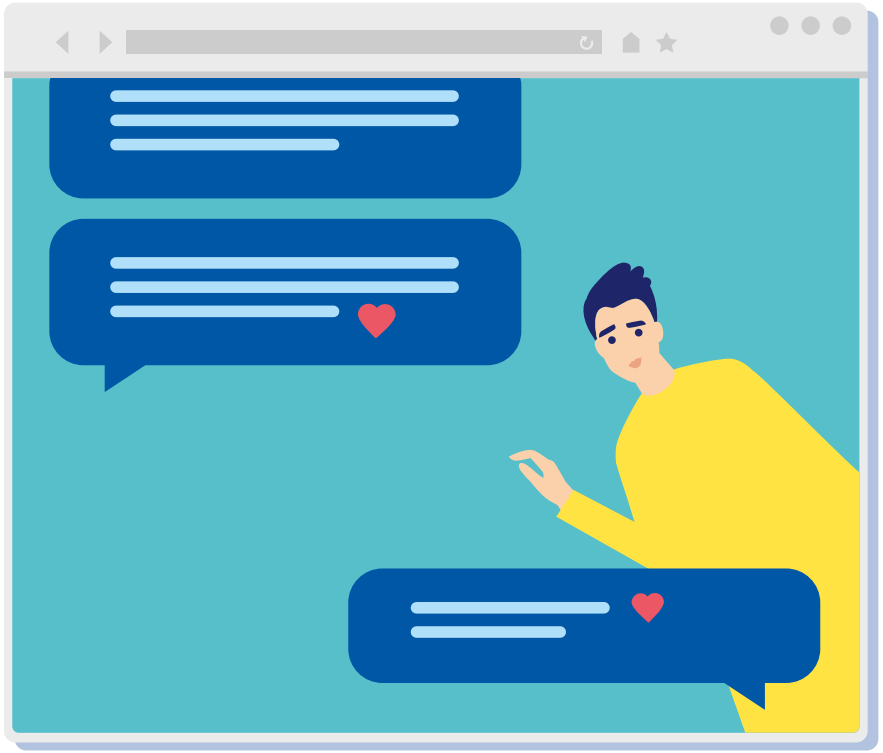
Das leere Geld-zurück-Versprechen

Refund Scam

- Überweisen Sie kein Geld an Anrufer oder Anruferinnen, die versprechen, Ihnen Geld zurückzugeben.
- Wenn Ihnen am Telefon Zeitdruck gemacht wird, werden Sie hellhörig und brechen Sie das Telefonat ab.

Betrügende Personen kontaktieren Sie telefonisch und behaupten, Geld gefunden zu haben und zurückzahlen zu wollen, das Sie bei einem vorherigen Investment verloren haben. Sie werden dazu aufgefordert, Gebühren zu bezahlen.

Druck machen für die Zahlung von Gebühren
Oft wird Ihnen zeitlicher Druck auferlegt. Zögern Sie, auf das Angebot einzugehen, wird Ihnen mit Anzeigen wegen Geldwäsche oder Konsequenzen durch die Polizei gedroht. Solange Sie aber die Gebühren bezahlen, erfinden die Betrügerinnen und Betrüger immer neue Gebühren oder Steuern. Sind Sie nicht mehr bereit zu zahlen, wird der Kontakt abgebrochen.



1

Der unbekannte Liebhaber

Romance Scam

Auf Social-Media-Plattformen wie Facebook, WhatsApp oder Instagram nehmen die Betrügerinnen und Betrüger Kontakt mit Ihnen auf. Dabei verstecken sie sich hinter einem besonders attraktiven Profil oder geben zum Beispiel vor, für ein humanitär tätiges Unternehmen oder als Soldat im Einsatz zu sein.

- **Seien Sie skeptisch bei Kontaktaufnahmen von Unbekannten über das Internet oder Smartphone.**

«Ich liebe dich und will mit dir zusammen sein!»

Mit Geschichten Vertrauen erschleichen
Die betrügenden Personen bauen über längere Zeit eine persönliche Beziehung mit Ihnen auf. Sie überschütten Sie mit Nettigkeiten, nehmen täglich Kontakt auf und täuschen Interesse an einer gemeinsamen Zukunft vor.

2

Geld für persönliche Notfälle anfragen
Ist die persönliche Beziehung eng genug aufgebaut, erfinden die Betrügerinnen und Betrüger persönliche Notfälle und bitten um Geld. Sie halten die Beziehung über lange Zeit aufrecht und erfinden immer wieder neue Notfälle, um Sie dazu zu bewegen, Geld zu überweisen.

- **Werden Sie hellhörig, wenn jemand für persönliche Notfälle Geld von Ihnen will.**
- **Überweisen Sie kein Geld an Personen, die Sie noch nie im echten Leben getroffen haben.**

3

Die falschen Familien-mitglieder

WhatsApp-Betrug

Sie erhalten eine WhatsApp-Nachricht oder SMS von einer unbekannten Nummer. Die Absenderin oder der Absender gibt vor, Ihr Sohn oder Ihre Tochter zu sein, deren Handy verloren gegangen oder kaputt ist.

„Hallo Mama, hier meine neue Nummer“

1

2

Finanzielle Hilfe per Nachricht anfragen
Nach einigen belanglosen Nachrichten verändert sich das Thema schnell zu einem dringenden Geldbedarf. Die angeblich verwandte Person könnte behaupten, dass eine Rechnung bis Ende des Monats bezahlt werden muss oder es gibt andere triftige Gründe für den schnellen Geldbedarf. Da das alte Handy defekt ist, sei der Zugang zum eBanking nicht möglich.

Bankdaten unter Zeitdruck
Sie werden gebeten, für eine dringende Zahlung Ihre Login-Daten für das eBanking zu übermitteln. Sobald die Betrügerin oder der Betrüger diese Information hat, versucht sie, ein eigenes Gerät für die Legitimierung zu registrieren, um Zugang zu Ihrem eBanking zu erhalten.

3

- **Lassen Sie sich nicht durch Dringlichkeit aus der Ruhe bringen. Kontaktieren Sie Ihre Kinder über die Ihnen bekannten Nummern.**
- **Geben Sie niemand anderem Zugang zu Ihrem Bankkonto.**
- **Falls Sie bereits Geld überwiesen haben, informieren Sie schnellstmöglich Ihre Bank.**

Der Schockanruf

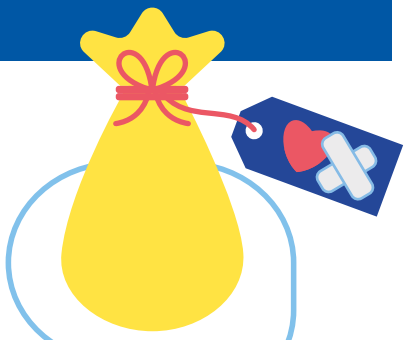
Telefonbetrug I

Sie bekommen einen Anruf und Ihnen wird mitgeteilt, dass zum Beispiel soeben ein schlimmer Unfall passiert ist. Am Telefon ist die Polizei oder eine Ihnen nahestehende Person, die beim Unfall schwer verletzt wurde. Für den Krankenhausaufenthalt oder eine Notoperation wird dringend Ihr Geld gebraucht.

Durch Notsituation einen Schock hervorrufen
Die betrügenden Personen geben sich als Polizei oder als die verletzte Person aus. Dabei kann auch eine technische Stimmverzerrung eingesetzt werden. Sie werden zur sofortigen Handlung aufgerufen. Denn in der Situation geht es um Leben und Tod. Die Betrügerinnen und Betrüger malen ein schlimmes Szenario und wollen Ihren Schockzustand ausnutzen.

Keine Zeit für Überprüfung
Die Geldübergabe muss dann möglichst schnell erfolgen. Dafür werden Sie von einem Taxi abgeholt oder eine Drittperson wird geschickt, das Geld bei Ihnen abzuholen. Nach der Übergabe ist das Geld weg und Sie finden heraus, dass es der nahestehenden Person gut geht und sie nicht in einen Unfall verwickelt ist.

- **Lassen Sie sich durch Dringlichkeit nicht aus der Ruhe bringen. Kontaktieren Sie die angeblich verunfallte Person.**
- **Für die Behandlung einer verunfallten Person ist nie eine Vorauszahlung nötig. Brechen Sie das Telefonat ab.**



Der falsche Polizist

Telefonbetrug II

Sie werden von der Polizei angerufen, weil Ihre Mithilfe in einem Fall wichtig ist. In der Nähe Ihres Wohnorts wird eine Person verdächtigt, eine Straftat begangen zu haben. Sie sollen helfen, der Person das Handwerk zu legen. Ausserdem ist es wichtig, dass Ihre Wertsachen sicher aufbewahrt werden, denn die Kriminellen in der Umgebung haben es auch auf Sie abgesehen.

Zusammenarbeit mit der Polizei
Die betrügenden Personen wollen sich Ihr Vertrauen erschleichen, indem sie andere Menschen des Betrugs beschuldigen und vorgeben, es hätte in der Umgebung einen Vorfall gegeben. Meist seien auch Bankmitarbeitende involviert, weshalb Sie die Bankangestellten keinesfalls kontaktieren dürfen.

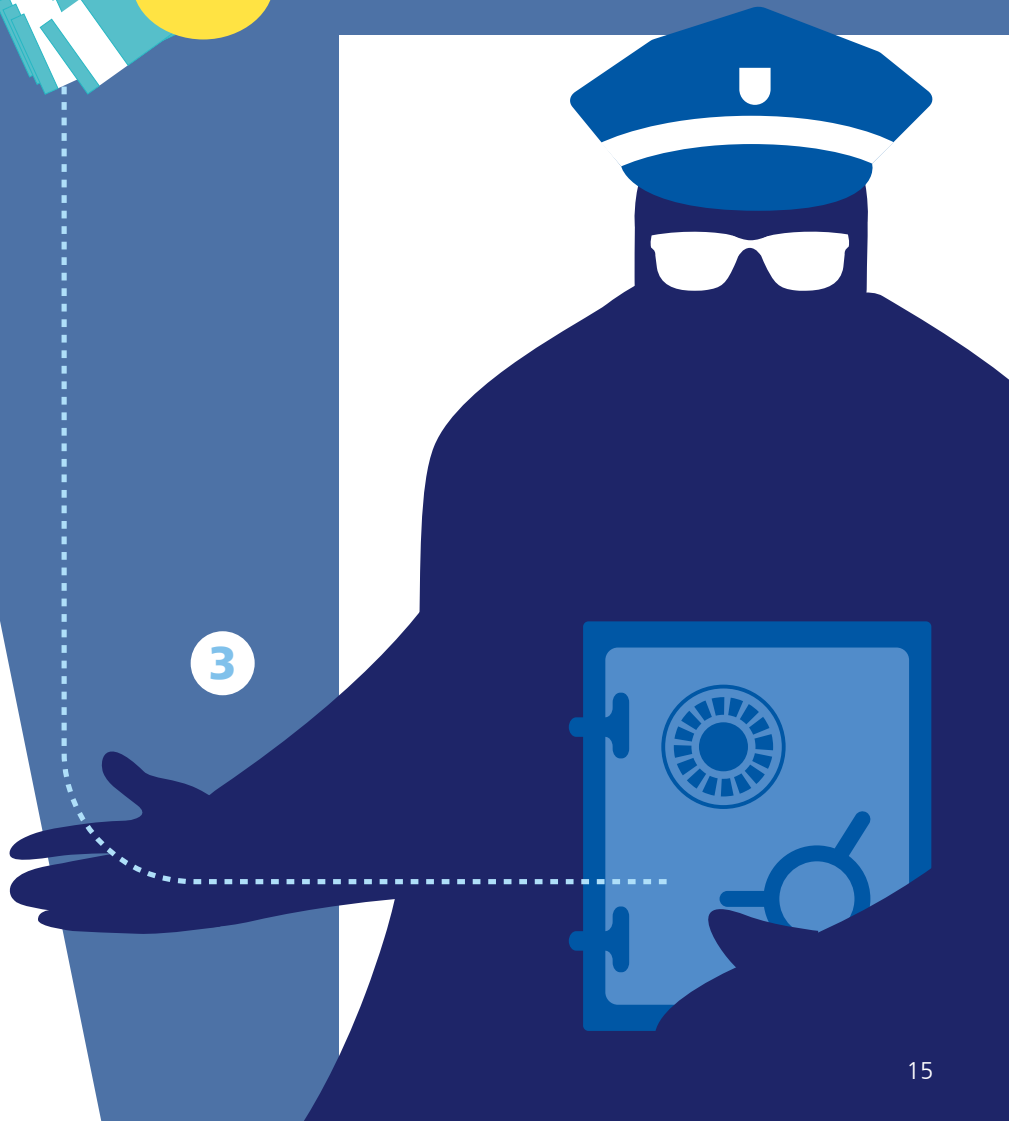
Ihr Freund und Helfer
Die angebliche Polizei möchte Ihnen helfen und Ihre Wertsachen in Sicherheit bringen. Eine Drittperson oder eine angebliche Polizistin oder ein Polizist in Zivilkleidung holt die Wertsachen und das Bargeld bei Ihnen ab. Haben Sie nichts zu Hause, werden Sie aufgefordert, zur Bank zu gehen. Dabei bekommen Sie auch Instruktionen, wie Sie sich gegenüber Mitarbeitenden der Bank zu verhalten haben.

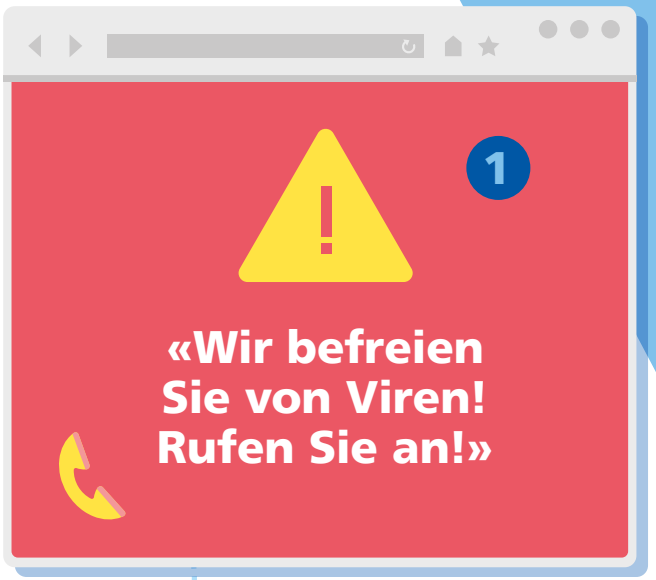
1

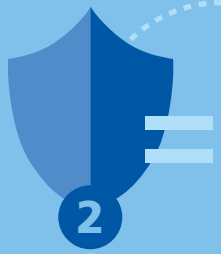
2

- Übergeben Sie niemals Wertsachen oder Bargeld der Polizei oder anderen Personen.
- Werden Sie hellhörig, wenn Sie über ein Telefonat nicht sprechen sollen.

3







Die trojanische Hilfe

Support Scam

Auf Ihrem Computerbildschirm erscheint die Nachricht, dass ein technischer Fehler aufgetreten ist oder Hacker auf Ihrem Computer sind. Sie werden aufgefordert, sofort eine eingeblendete Nummer anzurufen, um das Problem zu beheben.

Für den Support eine Software installieren
Die Betrügerinnen und Betrüger geben sich als Support-Mitarbeitende einer bekannten Technologiefirma, wie zum Beispiel Microsoft oder Amazon, aus. Sie werden am Telefon aufgefordert, eine Software zu installieren. Über diese Software verschaffen sich die Betrügerinnen und Betrüger uneingeschränkten Zugang zu Ihrem Computer mit der Möglichkeit, an persönliche Daten zu gelangen. Oft wird vorgegeben, dass das eBanking betroffen ist und Sie sich dazu einloggen müssen. Mit der Option, Ihren Bildschirm «auszuschalten», können dann betrügerische Zahlungen erfasst werden.

Für den Support eine Software mit langer Laufzeit verkaufen
Die Betrügerinnen und Betrüger geben vor, Ihnen ein Sicherheitsprogramm, zum Beispiel ein Antivirenprogramm, verkaufen zu wollen. Die Laufzeit beträgt meist mehrere Jahre oder gar lebenslang.

- **Holen Sie vertraulichen Rat ein vor dem Download fremder Software.**
- **Seien Sie wachsam bei Kaufaufforderungen.**

Betrügerische E-Mail

Phishing

Sie erhalten eine E-Mail mit der Aufforderung, auf einen Link zu klicken oder ein Dokument herunterzuladen.
Die E-Mail scheint auf den ersten Blick von einem bekannten Absender zu stammen, zum Beispiel Ihrer Arbeitgeberin oder Ihrem Arbeitgeber.

Sich Zugriff auf Daten und Systeme verschaffen
Hinter dem Link versteckt sich oftmals ein Formular, in das Sie persönliche Daten eingeben müssen, zum Beispiel ein Eingabefeld für Benutzernamen und Passwort. Hinter den Dokumenten im E-Mail-Anhang verstecken sich schädliche Programme, die Daten sammeln oder Systeme schädigen.

Persönliche Daten verkaufen oder Lösegeld fordern
Die Betrügerinnen und Betrüger wollen über die Links und die schädliche Software Ihre persönlichen Daten sammeln und verkaufen oder Ihr Computersystem so schädigen, dass Lösegeld für die Freigabe verlangt werden kann.

- **Öffnen Sie keine unerwarteten E-Mail-Anhänge.**
- **Tippen Sie für das Login Ihres eBankings immer die Website Ihrer Bank ein und klicken Sie nicht auf Anzeigen mit dem Hinweis «Werbung».**
- **Wenn Sie persönliche Informationen eingeben müssen, überprüfen Sie zuerst nochmals die Absenderadresse sowie den Link in der E-Mail.**
- **Wenn Sie unsicher sind, nehmen Sie anderweitig (zum Beispiel per Telefon) Kontakt auf mit dem vermeintlichen Absender.**

«Im Anhang finden Sie Ihre Telefonrechnung. Besten Dank für die fristgerechte Begleichung.»

Der gekaperte Computer

Malware

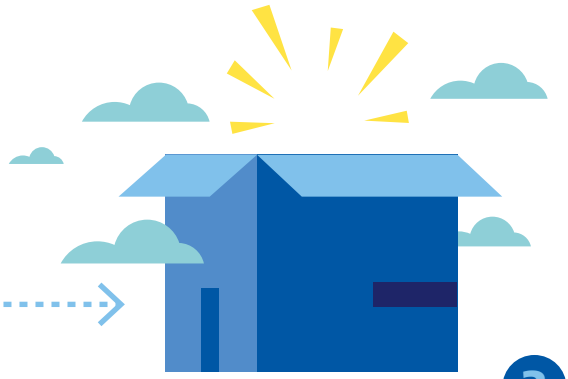
Betrügerinnen und Betrüger wollen auf Ihrem Computer eine Software installieren, um darauf zuzugreifen und Schaden anzurichten. Meist gelangt die schädliche Software (sogenannte Malware) über E-Mail-Anhänge, die heruntergeladen werden, auf Ihren Computer. Andere Mittel und Wege sind USB-Sticks oder Downloads, die unbemerkt im Hintergrund starten.

Die Software richtet unbemerkt Schaden an
Sobald sie installiert ist, kann sie unterschiedliche Ziele verfolgen:
- Daten verschlüsseln, um Lösegeld zu fordern
- Daten ausspionieren
- Tastenschläge aufzeichnen
- Datenströme umleiten usw.

Falscher Link zu täuschend echtem eBanking
Beim Bankentrojaner wird Ihnen eine E-Mail mit einem falschen Link geschickt. Klicken Sie darauf, werden am Computer Änderungen vorgenommen. Öffnen Sie das nächste Mal Ihre Bankverbindung, werden Sie auf eine falsche Internetseite weitergeleitet. Diese Seite sieht aus wie die echte Website Ihrer Bank und Sie loggen sich scheinbar wie gewohnt in Ihr eBanking ein.
So geben Sie Ihre Login-Informationen preis und die Betrügerinnen und Betrüger erhalten Zugang zu Ihrem eBanking.

- **Öffnen Sie keine unerwarteten E-Mail-Anhänge.**
- **Wenn Sie unsicher sind, nehmen Sie anderweitig (zum Beispiel per Telefon) Kontakt auf mit dem vermeintlichen Absender.**
- **Überprüfen Sie jeden Link in Ihren E-Mails, bevor Sie diese anklicken.**
- **Seien Sie vorsichtig, wenn Sie sich in Ihr eBanking einloggen. Überprüfen Sie die URL der Website.**

«Kaufen Sie den Mega-Deal! Nur noch 2 Stück auf Lager.»



3

Der leere Online-Kauf

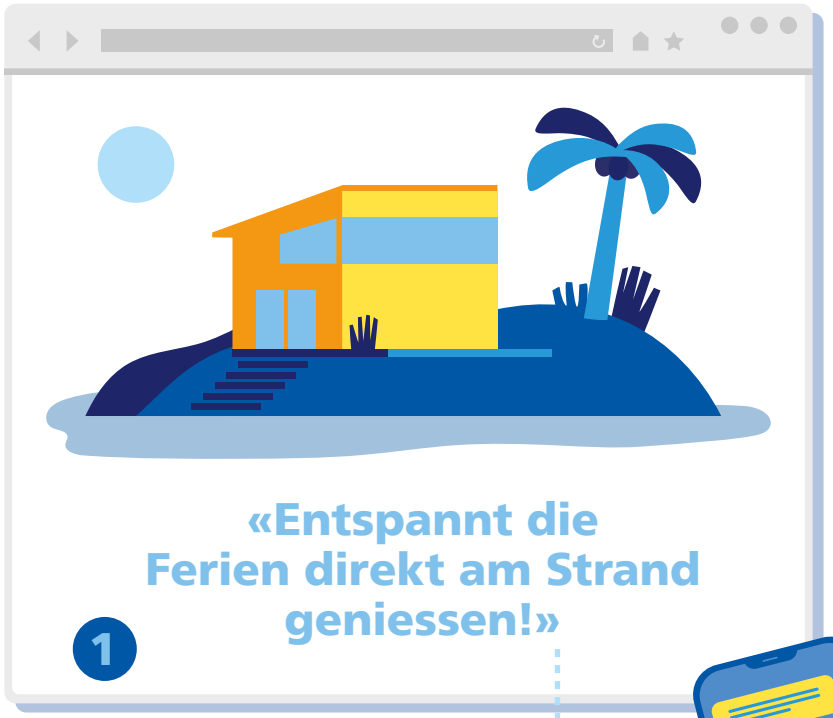
Shopping Scam

Sie sehen online ein gewünschtes Produkt zu einem attraktiven Preis. Bilder und Inserat suggerieren ein gutes Angebot und so nehmen Sie per E-Mail oder Chat den Kontakt auf.

Schnelle Zahlung für einmaliges Preis-Leistungs-Verhältnis
Die Betrügerinnen und Betrüger drängen auf eine schnelle Abwicklung des Geschäfts. Die Bezahlung erfolgt meist nicht über die Plattform, sondern über einen anderen Zahlungsabwickler. Sie sind vom Preis-Leistungs-Verhältnis sehr angetan und tätigen deshalb die Zahlung, wenn auch mit einem mulmigen Bauchgefühl.

Bestelltes Produkt existiert nicht
Nach der Zahlung brechen die Betrügerinnen und Betrüger den Kontakt zu Ihnen ab. Das bestellte Produkt kommt nie an und Ihr Geld ist weg.

- **Seien Sie skeptisch bei guten Angeboten, die nur kurzfristig erhältlich sind.**
- **Hören Sie auf Ihr Bauchgefühl, auch wenn (oder besonders wenn) das Angebot verlockend ist.**



Vermeintliche Ferienwohnung

Vorschussbetrug

Sie entdecken auf einer seriösen Online-Plattform ein Angebot für eine Ferienwohnung zu einem attraktiven Preis. Bilder und Inserat suggerieren ein gutes Angebot und Sie nehmen Kontakt auf.

Wechsel zu einem anderen Kommunikationskanal
Betrügende Personen wechseln oft schnell auf eine alternative Kommunikationsmethode wie E-Mail oder WhatsApp. Auf diesen neuen Kanälen werden Zahlungsinformationen ausgetauscht. Haben Sie bezahlt, bricht der Kontakt ab.

Ferienwohnung ist nicht vorzufinden
Wenn Sie schliesslich zur Ferienwohnung reisen, ist diese für Sie nicht zugänglich oder existiert gar nicht. Rückerstattungen für das bezahlte Geld sind fast nie möglich, da der offizielle Kommunikationsweg der Plattform verlassen wurde.

3

- **Kommunizieren Sie ausschliesslich über die offizielle Plattform, auf der inseriert wurde.**
- **Tätigen Sie Zahlungen nur über die offiziell vorgesehenen Kanäle auf der Plattform.**

Die falsche Zahlung

CEO Scam

Sie erhalten eine E-Mail, die auf den ersten Blick von Ihrer oder Ihrem Vorgesetzten oder vom CEO zu stammen scheint. In der E-Mail werden Sie aufgefordert, eine dringende Zahlung auszuführen.

Schnelle Zahlung unter Verschwiegenheit
Sie werden in der E-Mail zur Verschwiegenheit aufgefordert, da es sich um ein vertrauliches Geschäft oder Ähnliches handelt. Die E-Mail scheint häufig von einem bekannten Absender zu stammen, so erscheint im Absenderfeld der Name einer vorgesetzten Person. Diese Person ist meistens nicht erreichbar, wenn die E-Mail eintrifft, sodass keine Rücksprache gehalten werden kann.

Eine unauffällige Zahlung, die keinen Verdacht erregt
Um Abklärungen zu vermeiden, ist die Zahlung unauffällig in Bezug auf Betrag, Währung und Zielland. Die Visierungspflicht in Unternehmen in Kombination mit einer oftmals als dringend und vertraulich erfassten Zahlung kann die Kontrollmechanismen aushebeln und den Betrug begünstigen.

- **Werden Sie hellhörig bei Zeitdruck: Überprüfen Sie den Absender genau. Halten Sie Rücksprache mit verfügbaren Vorgesetzten.**
- **Lassen Sie eine Zahlung immer nach dem Vier-Augen-Prinzip kontrollieren.**

Der falsche Enkel

Enkeltrickbetrug

Sie erhalten einen Anruf einer unbekannten Person. Die Anruferin oder der Anrufer erschleicht sich im Laufe des Gesprächs den Namen eines oder einer Verwandten von Ihnen, zum Beispiel den Namen eines Enkels. Die Betrügerin oder der Betrüger gibt am Telefon vor, diese verwandte Person zu sein.

«Erkennst du mich? Ich bin's, dein Enkel.»

Fraudster:
"Albert, don't you recognise me? That makes me feel quite sad..."

You:
"Is that you Thomas?"

Fraudster:
"Of course, it's me – Thomas."

Am Telefon finanzielle Hilfe anfordern
Die Betrügerin oder der Betrüger am Telefon spricht auf sehr persönliche Weise mit Ihnen. Nach einem netten Gespräch kommt die anrufende Person darauf zu sprechen, dass sie dringend Hilfe braucht. Oft ist eine Investition oder ein Geschäft in Gefahr oder es gibt andere gute Gründe, warum die verwandte Person schnell Geld braucht.

Zeitdruck und Anweisungen für die Geldbeschaffung
Die betrügende Person drängt Sie dazu, noch am selben Tag Geld abzuheben.

Oft wird Ihnen genau vorgegeben, wie Sie das Geld abheben und die Fragen der Bankangestellten beantworten müssen.

Geldübergabe an einen «Freund»
Die Betrügerin oder der Betrüger gibt vor, das Geld nicht persönlich abholen zu können. Ihnen wird erzählt, dass eine vertraute Person das Geld abholen oder in Empfang nehmen wird. Sie werden gebeten, niemandem von der Transaktion zu erzählen. Ist das Geld an diese unbekannte Person übergeben, ist es verloren.

- **Übergeben Sie niemals Geld an unbekannte Personen.**
- **Werden Sie hellhörig, wenn Sie Geldgeschäfte geheim halten sollen. Sprechen Sie mit einer nahestehenden Person darüber.**
- **Wenn eine verwandte oder befreundete Person am Telefon von Ihnen Geld verlangt, bestehen Sie auf ein persönliches Treffen in einem Café oder Restaurant.**

Die fiktive Erbschaft

Erbschaftsbetrug

Sie werden von einer unbekannten Person telefonisch kontaktiert, die vorgibt, Notar, Erbin, Testamentsvollstrecker oder Ähnliches zu sein. Die Betrügerinnen und Betrüger gaukeln Ihnen vor …

- … dass eine entfernt verwandte Person verstorben ist und Ihnen eine beträchtliche Summe hinterlassen hat;
- … dass eine unbekannte Person verstorben ist und Ihnen zufällig viel Geld hinterlassen hat;
- … dass ein grosses Erbe auf Sie wartet, bei der Begleichung von Forderungen zur Auslösung der Erbschaft jedoch noch Ihre Unterstützung benötigt wird.

Geld für Anwälte und Anwältinnen, Gebühren oder Steuern
Um an die Erbschaft zu gelangen, werden Sie gebeten, Geld zu bezahlen. Mit diesem Geld bezahlen Sie angeblich eine Gebühr, die Kosten für eine Rechtsvertretung oder eine Steuerrechnung. Ihnen wird in Aussicht gestellt, dass Sie die Erbschaft erhalten, sobald der genannte Betrag überwiesen ist. Die angebliche Erbschaft wird jedoch nie ausbezahlt. Ihr Geld ist weg.

Kombination mit Romance Scam
Der Erbschaftstrick wird auch gerne in Kombination mit dem Romance Scam angewendet. Dabei gaukeln die betrügenden Personen Ihnen zuerst eine romantische Bindung vor und bitten Sie anschliessend um Hilfe, um eine Gebühr für den Antritt einer Erbschaft begleichen zu können. Sowohl die Gebühr als auch die Erbschaft (und die romantische Beziehung) existieren aber nicht.

«Sie haben Anspruch auf ein Erbe und können mit einer schönen Summe rechnen.»

- **Seien Sie skeptisch bei Kontaktaufnahmen von Unbekannten, die Ihnen Geld aus einer Erbschaft versprechen.**
- **Überweisen Sie kein Geld an Personen, die Sie noch nie im echten Leben getroffen haben oder deren Identität Sie nicht überprüfen können.**

Was können Sie tun?

Mit den Kenntnissen der Betrugsarten und mit etwas Vorsicht können wir gemeinsam dazu beitragen, versteckten Betrug zu entlarven und eine sicherere Umgebung für alle zu schaffen. Seien Sie wachsam, stellen Sie Fragen und überprüfen Sie die Informationen, bevor Sie Entscheidungen treffen oder persönliche Daten preisgeben.

Hier finden Sie Informationen und Unterstützung

Fachstelle eChannel Security
Telefon: 044 292 90 30
E-Mail: fachstelle_ecs@zkb.ch

Servicezeiten:
Montag bis Freitag: 8.00 bis 16.30 Uhr

eBanking Support
Kontaktieren Sie den Support direkt in Ihrem eBanking oder per Telefon: 0844 840 140
Auslandnummer: +41 44 293 95 95

Servicezeiten:
Montag bis Freitag: 8.00 bis 22.00 Uhr
Samstag / Sonntag: 9.00 bis 18.00 Uhr

Polizei
Bei Notfällen kontaktieren Sie direkt die Polizei.
Telefon: 117

Internet-Recherche
Informieren Sie sich bei den Fachstellen.
Finanzmarktaufsicht: www.finma.ch/de/finma-public/warnungen
Kantonspolizei ZH: www.cybercrimepolice.ch, www.telefonbetrug.ch
Nationales Zentrum für Cybersicherheit: www.ncsc.admin.ch
Hochschule Luzern «eBanking – aber sicher!»: www.ebas.ch

Rückfrage innerhalb Unternehmung
Tauschen Sie sich im professionellen Umfeld mit Ihren Kolleginnen und Kollegen sowie mit Vorgesetzten aus.

PC-Support
Falls Sie den Verdacht haben, dass Ihr Computer von einem Virus oder einer Schadsoftware betroffen ist, wenden Sie sich an einen professionellen PC-Support.

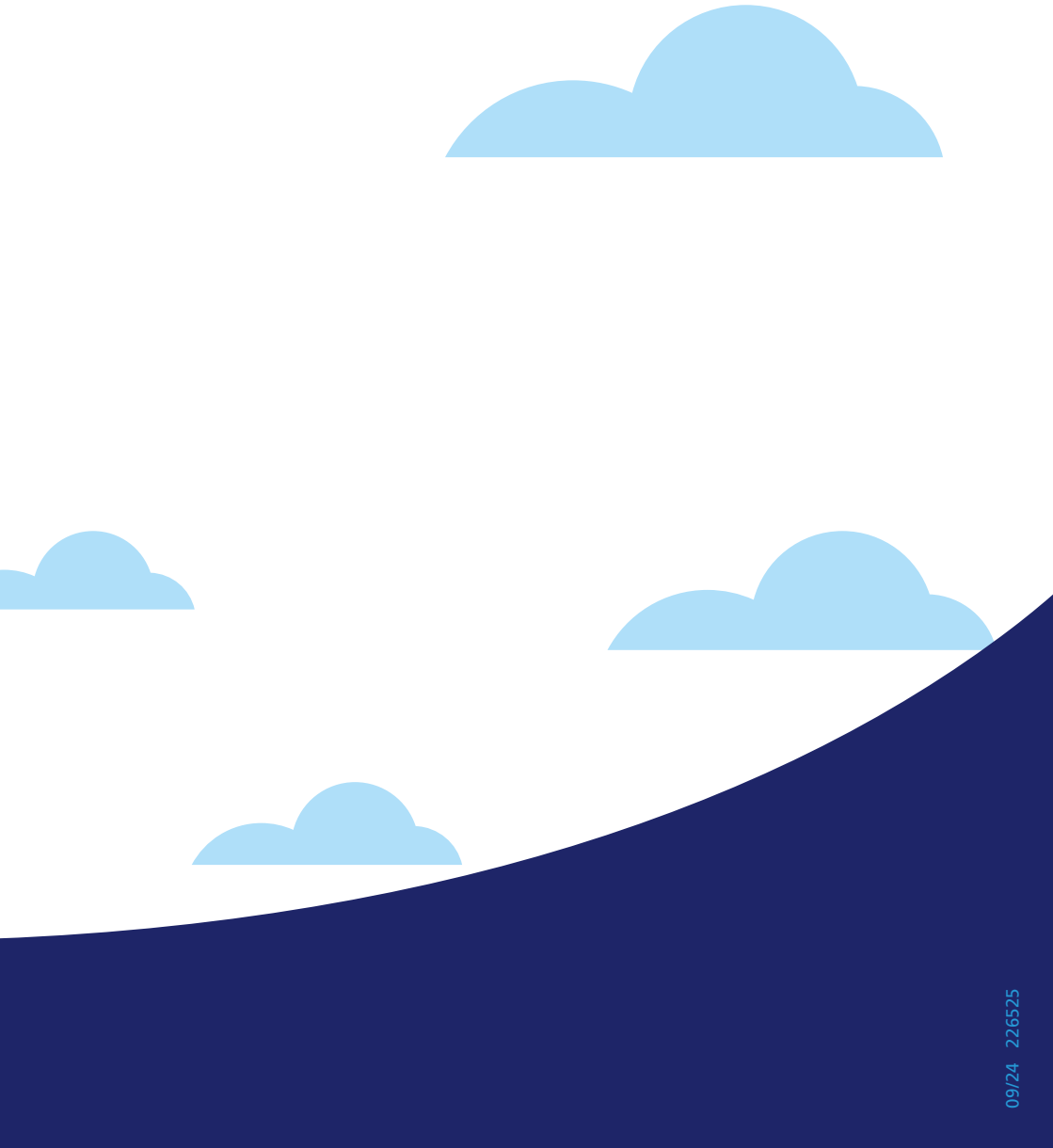
Freunde und Bekannte
Vertrauen Sie sich jemandem an und holen Sie sich Rat in Ihrem privaten Umfeld.

Notizen

Aktuelle Informationen zu verschiedenen Betrugsmaschen finden Sie auch online:

Unsere Website zkb.ch/betrug

Rechtliche Hinweise
Dieses Dokument dient ausschliesslich Informationszwecken. Bei den in dieser Broschüre behandelten Betrugsformen handelt es sich um eine Auswahl. Diese Broschüre ersetzt die einzelnen Produktverträge und -bestimmungen nicht. Die dortigen Risikohinweise und darin geregelten Sicherheitsvorkehrungen und Sorgfaltspflichten gelten für Sie als Kunde vorrangig.



09/24 226525