Bleiben Sie wachsam

Die gängigsten Betrugsmaschen kurz erklärt

Am richtigen Ort.ch

Aargauische Kantonalbank

Inhalt

Quishing	4
Falsche Bankmitarbeitende	4
Phishing	5
WhatsApp-Online-Betrug	5
Der falsche Support	6
Das schnelle Geld	6
Die grosse Liebe	7
Die kleinen Anzeigen	7
So verhalten Sie sich richtig	8
AKB-Podcast Finanz-Tanz	10

Bleiben Sie wachsam

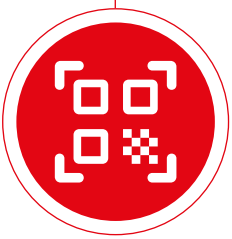
Betrugsfälle nehmen zu: Immer dreister werden die Betrügerinnen, Betrüger und ihre Maschen. Sie geben sich als Verwandte, Bekannte, Bankmitarbeitende, Staatsanwältin, Arzt oder als Polizistin aus und versuchen, mit verwirrenden und beängstigenden Geschichten das Vertrauen der Opfer zu gewinnen – und damit ihr Geld.

«Gemeinsam wachsam»: Unter diesem Slogan tritt die Aargauische Kantonalbank (AKB) mit der Kantonspolizei Aargau auf, wenn es ums Thema Betrugsprävention geht. «2024 wurden uns 207 Straftaten im Zusammenhang mit der Betrugsmasche Anlagebetrug gemeldet. Insgesamt überwiesen die 207 Opfer aus dem Kanton Aargau CHF 22 956 060.– ins Ausland», sagt Marco Dössegger von der Kantonspolizei Aargau.

Auch der AKB werden immer wieder Fälle von betrügerischen Anrufen und Betrugsmaschen gemeldet. Kriminelle nutzen sämtliche Kanäle und perfide Methoden, um ihre Opfer anzulocken und hinters Licht zu führen. Und obwohl sich die meisten Betrugsmaschen längst ins Internet verlagert haben, gibt es nach wie vor auch «analoge» Betrugsformen, also per Telefon, Brief oder persönlich an der Haustüre.

Bleiben Sie misstrauisch und wachsam, denn die Methoden werden mit den technischen Möglichkeiten immer raffinierter. In dieser Broschüre beschreiben wir die häufigsten Betrugsmaschen und -fälle und geben Ihnen wertvolle Tipps, wie Sie sich davor schützen können.

Quishing



Eine «beliebte» Internet-Betrugsmasche heisst «Quishing». Das Kofferwort steht für die Kombination der Begriffe «QR» und «Phishing». Kriminelle benutzen manipulierte QR-Codes, um ihre Opfer auf gefälschte Websites zu locken, wo sie sensible Informationen wie beispielsweise Passwörter eingeben sollen.
Dafür versenden die Betrügerinnen oder Betrüger eine E-Mail mit einer dringenden Aufforderung zum Handeln. Ein Beispiel: Sie könnten von Ihrer Bank aufgefordert werden, «sofort» einen QR-Code mit Ihrem Smartphone zu scannen und das Passwort Ihres Kontos zu ändern. Falls Sie das nicht tun, werde das Konto «aus Sicherheitsgründen» gesperrt.
Wenn Sie aber tatsächlich der Aufforderung Folge leisten, passiert genau das Gegenteil: Die Kriminellen gelangen in den Besitz Ihrer Login-Daten und haben Zugriff auf Ihr Konto.

Falsche Bankmitarbeitende

Es passiert leider immer wieder, dass Kriminelle sich als Mitarbeitende der AKB ausgeben. Sie teilen den Opfern mit, dass sich nächstens der technische Dienst der AKB melde, da verdächtige Aktivitäten auf dem Konto festgestellt wurden. Der Anruf folgt bald danach und es wird, oft in gebrochenem Deutsch, zu einer umgehenden Zahlung im e-Banking aufgefordert. Tun Sie das nicht! Die AKB ruft niemals Kundinnen und Kunden an, um solche Zahlungen zu verlangen. Geben Sie niemals persönliche Daten preis. Wenn Ihnen bei einem Telefongespräch mit einem sogenannten Bankmitarbeitenden etwas verdächtig vorkommt, legen Sie einfach auf. Das ist nicht unhöflich – es dient nur Ihrer Sicherheit. Rufen Sie sofort die Polizei (117) an.

Phishing

Mühsam, aber häufig: Gefälschte Suchmaschinen-Treffer im Internet verlinken auf betrügerische Online-Banking-Login-Seiten. Damit versuchen Cyber-Kriminelle, die Zugangsdaten für Ihr e-Banking zu stehlen. Suchen Sie das AKB e-Banking nie über Ihre Suchmaschine! So geht es richtig: Geben Sie von Hand unsere Website **www.akb.ch** in die Eingabezeile Ihres Internetbrowsers ein – oder die Adresse des AKB e-Bankings **eb.akb.ch.**

WhatsApp-Online-Betrug

Auf Messenger-Diensten wie WhatsApp kursieren betrügerische Jobangebote. Die Online-Kriminellen versuchen dabei, persönliche Informationen wie Adresse, Geburtsdatum und e-Banking-Kontodaten zu erlangen. Besonders dreist ist eine weitere Betrugsmasche: Sie erhalten eine WhatsApp-Nachricht oder SMS von einer unbekannten Nummer. Die Absenderin oder der Absender gibt vor, Ihr Sohn oder Ihre Tochter oder eine Ihnen vertraute Person zu sein, deren Handy verloren gegangen oder defekt ist. Nach einigen harmlosen Nachrichten folgt bald eine dringende Bitte um finanzielle Hilfe. Unter grossem Zeitdruck werden Sie aufgefordert, Ihre Bankdaten preiszugeben. Gehen Sie nicht darauf ein – brechen Sie den Kontakt sofort ab.

Der falsche Support

Betrügerinnen und Betrüger geben sich am Telefon gerne als Microsoft-Technikerinnen, -Techniker oder IT-Support aus und behaupten, Ihr Computer sei mit Viren infiziert oder habe Sicherheitsprobleme. Sie bieten Hilfe an und möchten per Fernzugriff auf Ihren Computer zugreifen. Dabei installieren sie Schadsoftware oder stehlen persönliche Daten. Manchmal verlangen sie auch Geld für angebliche Reparaturen oder Software. Wichtig: Microsoft ruft niemals unaufgefordert an! Legen Sie sofort auf. Gewähren Sie Fremden niemals Zugriff auf Ihren Computer.

Das schnelle Geld

Betrügerinnen und Betrüger werben online mit schnellem Geld und hohen Renditen. Leider werden für diese gefälschten Werbeanzeigen oft bekannte Persönlichkeiten missbräuchlich «eingesetzt». Das allein sollte Sie skeptisch machen. Sollten Sie dennoch auf die Werbung eingehen, werden sich die Kriminellen rasch bei Ihnen melden und Ihnen ihre Unterstützung anbieten – sogar bei der Kontoeröffnung. Sie werden aufgefordert, eine Kopie Ihres Passes oder Ihrer ID per Foto oder Scan zu übermitteln – angeblich zur «Verifizierung» – und eine erste Zahlung zu leisten. Tun Sie das nicht. Sie werden kein Geld verdienen. Im Gegenteil: Sie verlieren mit hoher Wahrscheinlichkeit Ihr Erspartes.

Die grosse Liebe

Wenn Sie – egal auf welcher Plattform – von unbekannten, meist ziemlich attraktiven Damen oder Herren angeschrieben werden, ist Vorsicht geboten. Leider ist gerade der sogenannte Romance-Scam eine der systematischsten Betrügereien mit Milliardengewinnen. Dahinter steckt das organisierte Verbrechen, und die Drehbücher, wie einsame Herzen auf gemeine Weise gekapert werden können, sind längstens und bestens erprobt. Warum sollten Sie Menschen, denen Sie noch nie begegnet sind (und die es gar nicht gibt), Geld überweisen? Lassen Sie sich nichts vormachen: Die Bilder sind gestohlen und die Lebensgeschichten von A bis Z gefälscht.

Die kleinen Anzeigen

Auch auf Kleinanzeigen-Portalen tummeln sich viele Betrügerinnen und Betrüger, die an Ihre Daten gelangen möchten. Bleiben Sie cool. Sie verkaufen. Sie haben die Kontrolle und bestimmen die Zahlungsmethode, das Tempo und die Abwicklung des Geschäftes. Wenn Sie nach dem Inserieren (achten Sie auf die holprige Sprache) kontaktiert werden von einer Person, die nicht in Ihrer Nähe (meistens im Ausland) wohnt und die bereits einen Kurierdienst oder die Post mit der Abwicklung des Geschäftes, inklusive der Zahlung, beauftragt hat, dann sollten bei Ihnen die Alarmglocken läuten. Ungewöhnliche Zahlungsmethoden können Sie vergessen. Screen-Shots, Links, QR-Codes, egal auf welchen Kanälen, auch wenn Sie noch so täuschend echt aussehen, sie sind gefälscht. Sie merken es, weil Sie in jedem Fall aufgefordert werden, Ihre Daten anzugeben. Tun Sie das nicht. Ihre Daten werden gestohlen und für weitere kriminelle Aktivitäten missbraucht.

So verhalten Sie sich richtig

Hier finden Sie einige wichtige und hilfreiche Regeln für den Umgang mit verdächtigen Situationen. Befolgen Sie diese konsequent und ohne schlechtes Gewissen – denn Ihr Gegenüber hat in der Regel keines.

Kontrollfragen stellen

Seien Sie misstrauisch bei Anrufen, bei denen Sie raten sollen, wer am Apparat ist. Stellen Sie gezielte Kontrollfragen wie: «Wann habe ich Geburtstag?»

Telefon auflegen

Wenn am Telefon Druck auf Sie ausgeübt wird: Legen Sie sofort auf. Das ist kein unhöfliches Verhalten, sondern aktiver Selbstschutz.

So dringend ist es nicht

Lassen Sie sich nicht durch vorgetäuschte Dringlichkeit aus der Ruhe bringen. Kontaktieren Sie im Zweifel direkt die angeblich verunfallte Person oder wenden Sie sich an die Polizei.

Geldforderungen ablehnen

Gehen Sie am Telefon nie auf Geldforderungen ein.

Keine Daten preisgeben

Geben Sie niemals persönliche Daten oder Passwörter an Personen weiter, die Sie unaufgefordert im Namen einer angeblichen «Behörde» anrufen.

Rücksprache halten

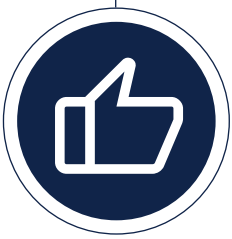
Sprechen Sie mit Personen aus Ihrem persönlichen Umfeld über das Geschehen. Lassen Sie sich – etwa bei Romance Scam – von niemandem einreden, dass Sie genau das nicht tun sollten.

Warnungen der Bank beachten

Nehmen Sie Warnungen von echten Bankmitarbeitenden ernst und akzeptieren Sie deren Hilfe.

Keine Übergabe

Übergeben Sie niemals Bargeld oder Wertsachen an unbekannte Personen!



In der 9. Staffel vom AKB-Finanzpodcast dreht sich alles um Kriminal-Prävention. Zu Gast ist Marco Dössegger von der Kantonspolizei Aargau. Er spricht über die verschiedenen Methoden und Vorgehensweisen, die Menschen mit krimineller Energie nutzen, um ans Geld ihrer potenziellen Opfer zu gelangen. Dabei spielt das Banking eine entscheidende Rolle. Im Gespräch mit Andrin Willi erklärt Marco Dössegger, wie man die Tricks der Betrügerinnen und Betrüger erkennt, wie man darauf reagieren und was man nicht tun sollte.

Jetzt reinhören:
akb.ch/podcast-betrug

e-Banking, aber sicher!

Egal ob Anfängerinnen, Anfänger oder Fortgeschrittene – lernen Sie, Ihre Daten und Geräte zu schützen und das Internet und e-Banking sicher zu nutzen. Jetzt zum Onlinekurs («eBanking – aber sicher!») der Hochschule Luzern (HSLU) anmelden:

ebas.ch/kursuebersicht

5001	**Aarau**	Tel. 062 835 77 77
5401	**Baden**	Tel. 056 556 66 01
5242	**Birr-Lupfig**	Tel. 056 464 20 80
5620	**Bremgarten**	Tel. 056 648 28 88
4805	**Brittnau**	Tel. 062 745 88 44
5200	**Brugg**	Tel. 056 448 95 95
5312	**Döttingen**	Tel. 056 268 61 11
5442	**Fislisbach**	Tel. 056 204 22 00
5070	**Frick**	Tel. 062 871 68 78
5722	**Gränichen**	Tel. 062 855 50 80
5080	**Laufenburg**	Tel. 062 874 42 62
5600	**Lenzburg**	Tel. 062 888 50 60
4312	**Magden**	Tel. 061 843 73 00
5507	**Mellingen**	Tel. 056 491 90 00
4313	**Möhlin**	Tel. 061 853 73 00
5630	**Muri**	Tel. 056 675 80 80
8965	**Mutschellen**	Tel. 056 648 24 24
5415	**Nussbaumen**	Tel. 056 296 20 20
5036	**Oberentfelden**	Tel. 062 738 33 33
4665	**Oftringen**	Tel. 062 553 55 89
4600	**Olten**	Tel. 062 207 99 99
5734	**Reinach**	Tel. 062 765 80 50
4310	**Rheinfelden**	Tel. 061 836 31 31
4852	**Rothrist**	Tel. 062 785 60 85
5707	**Seengen**	Tel. 062 767 90 80
5643	**Sins**	Tel. 041 789 71 11
8957	**Spreitenbach**	Tel. 056 555 70 55
5034	**Suhr**	Tel. 062 842 89 89
5430	**Wettingen**	Tel. 056 437 33 33
5103	**Wildegg**	Tel. 062 893 36 36
5610	**Wohlen**	Tel. 056 619 95 11
4800	**Zofingen**	Tel. 062 745 81 11

Stand Oktober 2025. Änderungen sind jederzeit möglich.

akb.ch/betrug

Am richtigen Ort.ch

Aargauische Kantonalbank