

**Sicherheit beim Digitalen Banking und
Schutz vor finanziellen Betrugsversuchen**

10. & 11. September 2025



BEKB

BCBE

Zu meiner Person



- **Florian Bachofner**
- **Wohnhaft in Belp**
- **22 Jahre Berner Kantonalbank AG**
- **Betriebsökonom MScBA**



Finanzmissbrauch in Zahlen

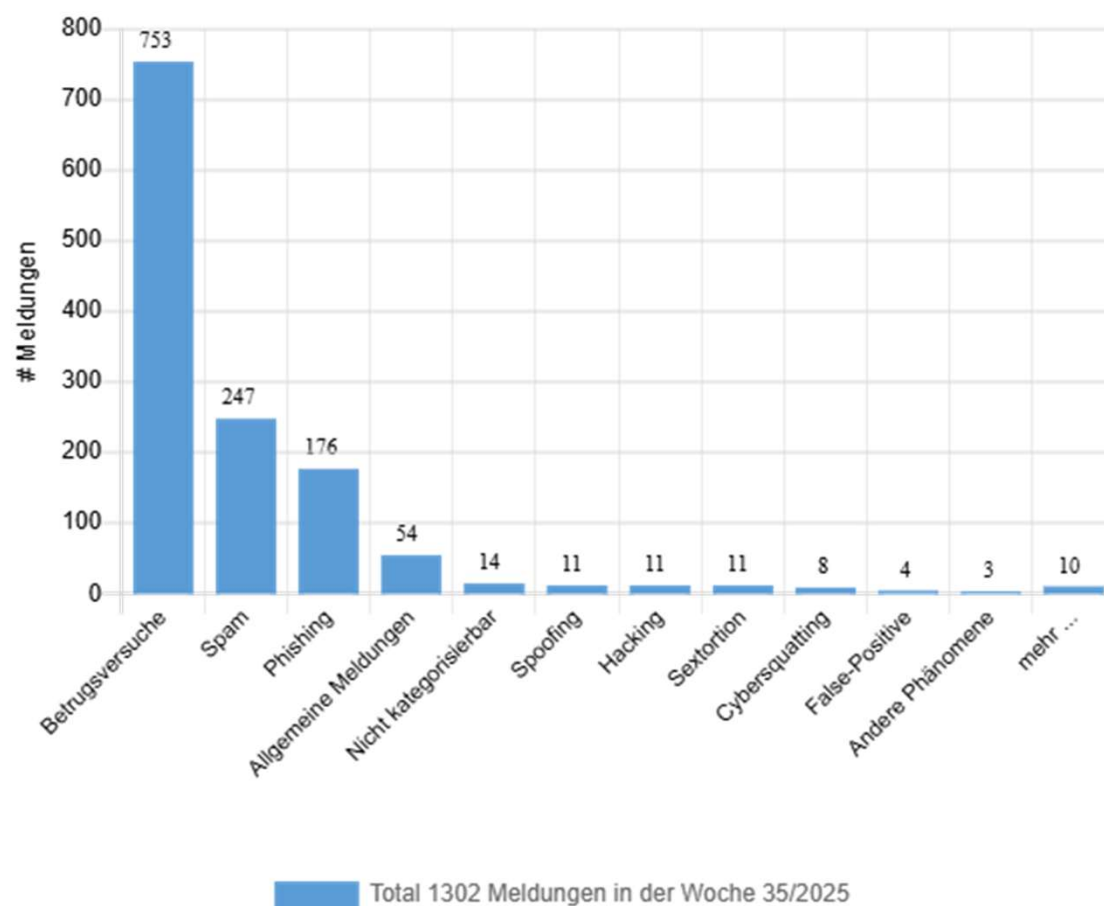
Jede fünfte Person im Alter über 55 Jahren erlitt in den vergangenen fünf Jahren finanziellen Missbrauch. Die Schadenssumme lag 2023 im Jahresschnitt um zwei Drittel höher als 2018 (+68.75%).

	2018	2023
Schaden (CHF)	400 Mio.	675 Mio.
Geschädigte	25.5%	19.8%
Betrugsversuche	73.8%	78.3%

	TOP 5
	Kostspieligste Missbrauchsformen
255 Mio.:	Berufstätige, die ihre Position missbrauchen
216 Mio.:	Missbrauch einer Vollmacht/ Zugang zu Bankkonto
47 Mio.:	Betrügerische Investitionen
36 Mio.:	Rechnung für nicht gekaufte Ware oder Dienstleistung
28 Mio.:	Waren und Dienstleistungen zu hohen Preisen

www.prosenectute.ch

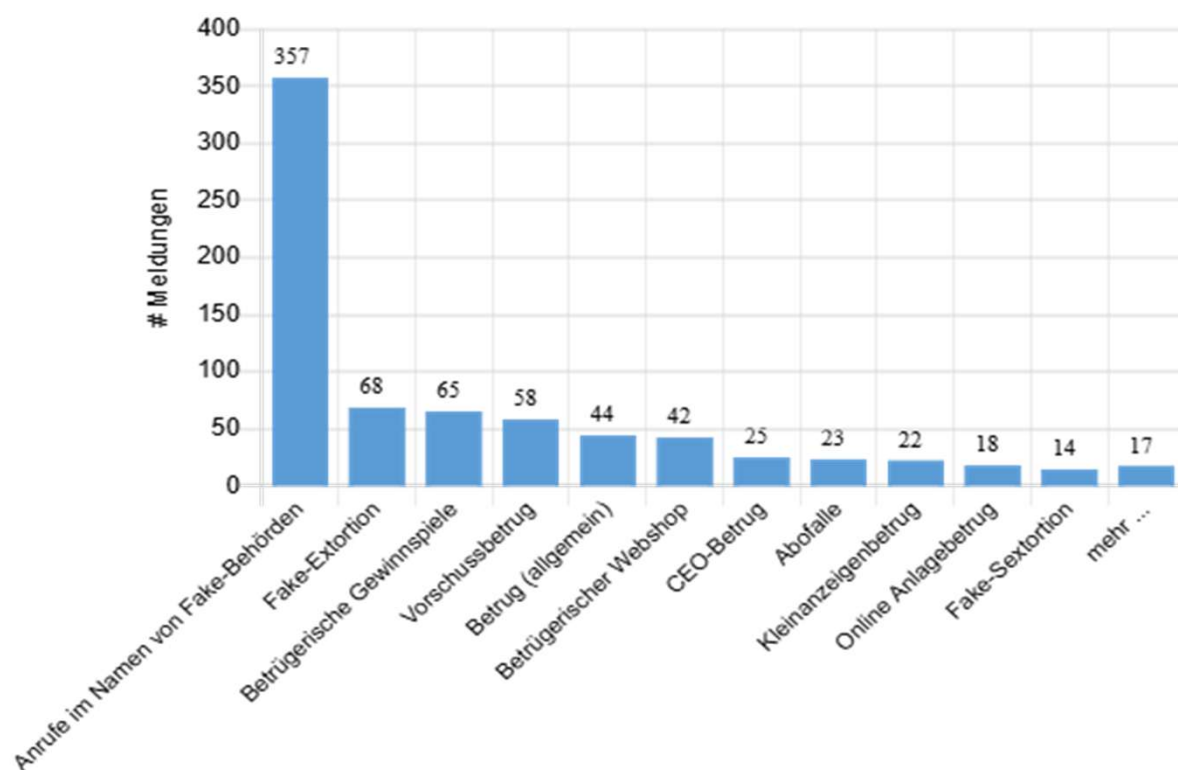
Finanzmissbrauch in Zahlen



Meldeeingang nach Hauptkategorien:
Woche 35/2025

www.ncsc.admin.ch

Finanzmissbrauch in Zahlen



753 Meldungen in der Hauptkategorie Betrugsversuche in der Woche 35/2025

Meldeeingang nach Unterkategorien
in der Hauptkategorie Betrugsversuche:
Woche 35/2025

www.ncsc.admin.ch

Typische Betrugsformen im Finanzbereich

Telefonbetrug «Enkeltrick»

Beim Enkeltrick-Betrug handelt es sich um eine Form von Telefonbetrug. Dabei wird vorgetäuscht, dass sich am anderen Ende ein Verwandter oder naher Bekannter befindet, der in finanziellen Nöten steckt und Sie um Hilfe bittet.

Telefonbetrug «Schockanruf»

Bei diesem wird vorgegaukelt, dass ein nahes Familienmitglied in einen Unfall verwickelt ist und nun in Untersuchungshaft kommt. Um dies zu verhindern, soll ein grösserer Geldbetrag als Kautions hinterlegt werden.

Typische Betrugsformen im Finanzbereich

Telefonbetrug «Falscher Polizist» oder «Falscher Sicherheitsdienst»

Bei diesem Telefonbetrug geben sich die Täter als Polizisten aus und bitten um Hilfe, einen vermeintlichen Betrüger in die Falle zu locken. Der Betrug endet mit einer Übergabe der Beute an den falschen Polizisten, an einen Kurier der Polizei oder an die Staatsanwaltschaft. Übergeben Sie nie Bargeld an unbekannte Personen.

Support-Telefonbetrug

Die Täter rufen Sie unter dem Vorwand an, Ihnen bei einem wichtigen Fehler zu helfen. Zum Beispiel falsche «Microsoft-Spezialisten» für Ihr Windows. Nachdem Sie die Kontrolle über Ihren Computer übernommen haben, folgen Geldforderungen, etwa zum Beheben des «gravierenden Fehlers» – oder Ihre Daten werden als Geisel genommen.

Typische Betrugsformen im Finanzbereich

Anrufe im Namen von falschen Behörden

«Guten Tag, hier ist die Sicherheitsabteilung Ihrer Bank»

... erhält das NCSC immer wieder Meldungen zu Telefonanrufen von angeblichen Bankmitarbeitenden, die vorgeben, bei der Sicherheitsabteilung zu arbeiten. Die Anrufer behaupten, dass sie eine betrügerische Zahlung stoppen wollen. Die angezeigte Telefonnummer entspricht der offiziellen Nummer der Bank. Diese wird von den Betrügern gefälscht/gespoofed, um glaubwürdig zu erscheinen.

«Haben Sie einen Flachbildschirm gekauft?»

In den letzten Wochen wurden dem NCSC vermehrt Anrufe von angeblichen Bankmitarbeitern gemeldet, die sich danach erkundigen, ob der Angerufene tatsächlich eine Zahlung getätigt habe. In vielen Fällen wird z. B. behauptet, dass eine Abbuchung für einen Flachbildschirm in einem Elektronikmarkt vorliege.

www.ncsc.admin.ch

Erkennen von betrügerischen Anrufen

- Die echte Polizei fordert niemals, dass Bargeld oder Wertsachen übergeben oder hinterlegt werden;
- Es werden keine Seriennummern von Banknoten am Telefon abgefragt;
- Es werden keine Kautionen oder Vorauszahlungen bei Verkehrsunfällen oder ähnlichen Ereignissen verlangt;
- Übergeben Sie niemals Bargeld oder Schmuck an unbekannte Personen;
- Seien Sie misstrauisch, wenn angebliche Verwandte oder Behörden Geld verlangen;
- Rufen Sie vermeintlich betroffene Angehörige direkt unter der Ihnen bekannten Nummer zurück;
- Nutzen Sie im Zweifel die bekannten Telefonnummern oder E-Mail-Adressen Ihres Bankberaters, um Rücksprache zu halten.

Typische Betrugsformen im Finanzbereich

Betrügerische Internetshops

Cyberkriminelle betreiben im Internet betrügerische Shops, um sich unrechtmässig zu bereichern. Waren werden Ihnen in schlechter Qualität oder gar nicht geliefert. Ihre hinterlegten Kreditkarteninfos könnten gefährdet sein – wenn es denn Betrügern z.B. nur darum geht, mit einem Fake-Shop an Kreditkartendaten zu gelangen.



Typische Betrugsformen im Finanzbereich

Gefälschte Loginseiten für eBanking oder Twint

Durch gefälschte E-Banking Login-Seiten im Internet versuchen Betrüger, Ihre Zugangsdaten zu stehlen und Zugriff auf Ihr Konto zu erlangen.

Falsche QR Codes bei Verkäufen auf Onlineplattformen (Tutti, Ricardo). Wenn ich Geld erhalten soll, muss ich nie irgendwo meine Logindaten eingeben oder 2FA bestätigen.

Kartenmissbrauch

bei Online-Shopping oder durch unvorsichtige Herausgabe von Kartendaten.

Sichere Nutzung von E-Banking und Mobile Banking

Durch bewusstes Handeln und die Anwendung von einfachen Sicherheitsmassnahmen ist ein sicheres E-Banking-Erlebnis gewährleistet.

- Nur den direkten Weg über die offizielle Bank-App oder die richtige Webseite nutzen, nie über Suchmaschine, Links in E-Mails oder SMS;
- Ihre Bank verschickt niemals E-Mails oder sonstige Nachrichten, die Sie auffordern, auf einen Link zu klicken und sich für das E-Banking anzumelden;
- Login immer mit Zwei-Faktor-Authentisierung absichern (z. B. Mobile App, SMS-Code).
- Nutzen Sie jeweils nur Ihre E-Banking-Seite und öffnen Sie keine anderen Internetseiten, solange Sie im E-Banking sind;

Sichere Nutzung von E-Banking und Mobile Banking

- Kontrollieren Sie auf Ihrer Login-Seite, ob Ihre Verbindung sicher ist. Das erkennen Sie, je nach Browser, am Schloss-Symbol in der Adresszeile oder in der Statuszeile ganz unten links;
- Zahlungen prüfen – Vor dem Freigeben Empfänger, IBAN und Betrag nochmals kontrollieren, besonders bei neuen oder geänderten Rechnungen;
- Prüfen Sie genau, was Sie auf Ihrer App bestätigen. Bestätigen Sie nie eine Zahlung, die Sie nicht selbst erfasst haben;
- Melden Sie sich stets mit «Abmelden» ab, sobald Sie fertig sind.



Sichere Nutzung von Bankkarten

- Lernen Sie Ihre Karten-PIN auswendig und behalten Sie sie immer für sich. Vermeiden Sie offensichtliche Kombinationen wie Ihr Geburtsdatum oder das Ihrer Kinder. Die Bank wird Sie nie auffordern, Ihre PIN bekanntzugeben. Geben Sie die PIN auch nie an Türöffner-Kästchen mit Tastaturen ein, falls dazu aufgefordert;
- Ob beim Geld abheben, bezahlen oder Billett lösen: Geben Sie ihre PIN immer verdeckt ein und lassen Sie sich dabei nicht von anderen Personen helfen oder ablenken. Nehmen Sie keine Hilfe an, wenn Ihre Karte feststecken sollte, sondern melden Sie das Ihrer Bank;
- Merken Sie sich das Aussehen der Geldautomaten. Sollte etwas daran anders sein (z.B. verdächtiger Aufsatz) beziehen Sie dort kein Geld und verständigen Sie die Bank. Geben Sie Ihrer Karte auch nicht aus der Hand, wenn (Verkaufs-) Personen Sie darum bitten. Sie könnten ausgetauscht werden;
- Speichern Sie die Notfallnummer Ihres Kartenherausgebers auf dem Mobiltelefon.

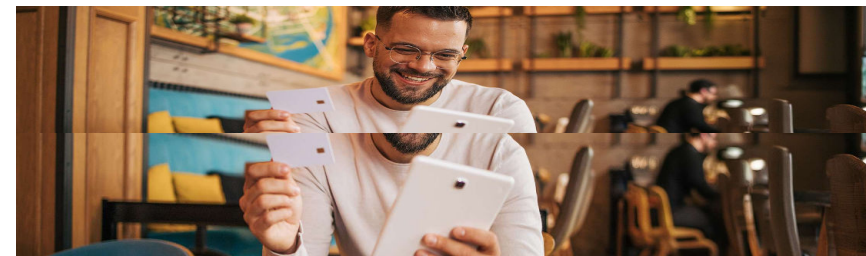


Verhalten im Verdachts- oder Schadensfall

- Kontaktieren Sie Ihre Bank bei verdächtigem Verhalten im E-Banking (z.B. Anzeige eines Timers oder einer Sanduhr) oder fragwürdigen Zahlungen unverzüglich. Sie kann Zahlungen stoppen oder Rückrufe prüfen;
- Im Finanzbereich ist Ihre Bank die erste Ansprechperson. Danach Polizei involvieren;
- Zugang zum E-Banking sofort sperren lassen und Karten und Twint blockieren;
- Verdächtige Webseiten können direkt dem BACS auf antiphishing.ch gemeldet werden;
- Sperren Sie Ihre Karte bei Verdacht auf Missbrauch. Dasselbe gilt bei Diebstahl, Verlust oder nach Einzug an einem Automaten;
- Brechen Sie verdächtige Anrufe sofort ab (insbesondere wenn Druck auf Sie ausgeübt wird) und melden Sie diese der Polizei über die Notrufnummern 117 oder 112. Ignorieren Sie auch sämtliche Mails/Nachrichten von betrügerischen Anrufern.
Falls Sie unsicher sind, rufen Sie auf die offiziellen Bank-Nummern an.

Präventive Unterstützung durch die Bank

- Transaktionsüberwachung im Hintergrund (Transaktionssignierung, verdächtige Zahlungen werden blockiert oder abgefragt);
- Tages- und Kartenlimiten einrichten – so wird ein möglicher Schaden begrenzt;
- Push-Nachrichten oder SMS-Benachrichtigungen aktivieren, damit der Kontoinhaber sofort über Belastungen informiert wird;
- Der Bankkunde bleibt verantwortlich für seine Zugangsdaten und alle Aktivitäten in seinem eBanking;
- Die Kundinnen und Kunden sind nicht auf sich allein gestellt – die Bank unterstützt aktiv, sowohl vorbeugend als auch im Ernstfall.





**Herzlichen Dank und bleiben Sie
informiert und wachsam**



BEKB

BCBE