



INFO-BLATT N°2

Sicherheit & Betrug

Wie schütze ich mich?

Betrüger zielen oft auf Senioren ab. Dieses Blatt hilft Ihnen, sie zu erkennen und sich zu schützen.

Jedes Jahr werden in der Schweiz Tausende von Menschen per Telefon, E-Mail oder SMS betrogen. Senioren sind besonders gefährdet — nicht weil sie naiv sind, sondern weil Betrüger sehr professionell vorgehen. Die Methoden zu kennen, ist bereits der halbe Schutz.

! Die häufigsten Betrugsmaschen



Gefälschter IT-Support

● **SEHR VERBREITET IN DER SCHWEIZ**

Sie erhalten einen Anruf von einer Person, die sich als Techniker von **Microsoft, Apple oder Swisscom** ausgibt. Sie sagt, Ihr Computer sei mit einem Virus infiziert und sie müsse ihn ferngesteuert reparieren.

💬 *Was sie sagen: "Guten Tag, ich rufe von Microsoft an. Wir haben einen Virus auf Ihrem Computer entdeckt. Ich muss Ihr Gerät fernsteuern, um Ihnen zu helfen."*



Microsoft, Apple und Swisscom rufen Sie NIEMALS spontan an.

Legen Sie sofort auf. Geben Sie einem Unbekannten niemals Zugriff auf Ihren Computer.



Gefälschter Bankangestellter

● STARK ZUNEHMEND

Jemand gibt sich als Bankangestellter aus und sagt, Ihr Konto wurde gehackt. Er verlangt Ihre Codes, Passwörter oder eine Überweisung auf ein "sicheres Konto".

💬 Was sie sagen: "Guten Tag, ich bin von der PostFinance. Ihr Konto ist in Gefahr. Um es zu schützen, brauche ich jetzt Ihren SMS-Code."

- ✅ Ihre Bank wird Sie NIEMALS nach Ihrem SMS-Code oder Passwort fragen. Legen Sie auf und rufen Sie Ihre Bank direkt über die Nummer auf der Rückseite Ihrer Karte an.



Gefälschte Liefer-SMS

● SEHR HÄUFIG PER SMS UND E-MAIL

Sie erhalten eine SMS oder E-Mail, die besagt, dass ein Paket auf Sie wartet und Sie Zollgebühren bezahlen oder auf einen Link klicken müssen, um die Lieferung zu bestätigen.

💬 Was sie schreiben: "Ihr Paket N°CH8492 wartet. Zahlen Sie CHF 2.50 Liefergebühren hier: [verdächtiger Link]"

- ✅ Klicken Sie niemals auf einen per SMS erhaltenen Link. Wenn Sie ein Paket erwarten, gehen Sie direkt auf die Website der Post oder DHL, indem Sie die Adresse selbst eingeben.



Romantikbetrug ("Romance Scam")

● OFT SEHR SCHWER ZU ERKENNEN

Eine Person kontaktiert Sie über soziale Medien oder E-Mail. Sie ist charmant, aufmerksam und gibt an, sich zu verlieben. Nach einigen Wochen bittet sie Sie um Geld für einen Notfall.

💬 Was sie sagen: "Ich muss so schnell wie möglich von meinem Einsatz zurückkehren, um Sie zu sehen, aber ich brauche CHF 500 für das Ticket. Ich erstatte es Ihnen bei meiner Ankunft."

- ✅ Überweisen Sie niemals Geld an jemanden, den Sie nie persönlich getroffen haben. Sprechen Sie zuerst mit einer Vertrauensperson.



Gefälschter Gewinn / Lotterie

● KLASSISCH ABER NOCH WIRKSAM

Sie erhalten eine Nachricht, dass Sie einen Preis gewonnen haben (Auto, Reise, Geldbetrag). Um ihn zu erhalten, werden Sie gebeten, "Verwaltungsgebühren" zu zahlen.

 Was sie schreiben: "Herzlichen Glückwunsch! Sie wurden ausgewählt, CHF 15'000 zu gewinnen. Um Ihren Gewinn zu erhalten, zahlen Sie bitte CHF 50 Bearbeitungsgebühr."

- ✓ **Man zahlt nie, um einen Gewinn zu erhalten.** Wenn Sie nicht an einem Gewinnspiel teilgenommen haben, können Sie keines gewonnen haben. Ignorieren und löschen.



Die 6 goldenen Regeln von SeniorPhone

1 Geben Sie Ihre Passwörter oder Codes niemals weiter

Weder per Telefon, noch per E-Mail, noch per SMS — niemals, an niemanden, unter keinem Vorwand.

2 Klicken Sie niemals auf einen per SMS erhaltenen Link

Geben Sie die Website-Adresse immer selbst in Ihren Browser ein.

3 Im Zweifel auflegen und selbst zurückrufen

Verwenden Sie die offizielle Nummer auf der Rückseite Ihrer Bankkarte oder auf der offiziellen Website.

4 Überweisen Sie niemals Geld unter Druck

Echte finanzielle Notfälle lassen sich überprüfen. Nehmen Sie sich Zeit zum Nachdenken und sprechen Sie mit einem Angehörigen.

5 Geben Sie einem Unbekannten niemals Zugriff auf Ihren Computer

Microsoft, Apple und Swisscom rufen Sie niemals spontan an, um Ihnen zu helfen.

6 Sprechen Sie zuerst mit einer Vertrauensperson

Ein Blick von aussen hilft oft, einen Betrug zu erkennen, den man selbst nicht gesehen hat.

Was tun bei einem verdächtigen Anruf?

Unterdrückte Nummer

Ihr Bildschirm zeigt "*Unterdrückt*" oder "*Unbekannt*" — die Person verbirgt absichtlich ihre Identität.

Nicht abnehmen. Auflegen.

Unbekannte Nummer

Sie erkennen die Nummer nicht. Klingeln lassen. Wenn es wichtig ist, hinterlässt die Person eine Voicemail.

Warten. Nur zurückrufen bei Nachricht.

 **Attention aux numéros 0900** — ce sont des numéros surtaxés qui vous coûtent plusieurs francs par minute. Ne rappelez jamais un numéro commençant par **0900** si vous ne savez pas à qui il appartient.

Das Wichtigste

- Betrug per Telefon, SMS und E-Mail ist sehr professionell — es ist keine Frage der Naivität.
- Weder Ihre Bank, noch Microsoft, noch Swisscom werden jemals Ihre Codes verlangen.
- Im Zweifel: auflegen, nachdenken, eine Vertrauensperson anrufen.
- Klicken Sie niemals auf einen per SMS erhaltenen Link, même s'il semble officiel.
- Sie können einen Betrug bei der Kantonspolizei oder auf cybercrime.ch melden.



Warnung der Kantonspolizei Genf — Juni 2026

Betrüger verteilen in Briefkästen **gefälschte Benachrichtigungszettel**, die perfekt die echten der Schweizerischen Post imitieren. Das Dokument ist extrem glaubwürdig.



Wie der Betrug funktioniert:

- 1 Sie erhalten einen gefälschten Post-Benachrichtigungszettel im Briefkasten
- 2 Er fordert Sie auf, einen QR-Code zu scannen, um "Ihre Lieferung neu zu planen"
- 3 Der QR-Code führt zu einer **gefälschten Website**, die genau wie die Post aussieht
- 4 Sie werden nach Ihren Daten und einer Zahlung von CHF 2.10 "Gebühren" gefragt
- 5 **Echtes Ziel: Ihre Kreditkartendaten stehlen!**



Unbedingt merken:

- Die Post verlangt **NIE eine Zahlung per QR-Code** für eine Lieferung
- Scannen Sie **nie einen QR-Code** aus dem Briefkasten ohne Überprüfung
- Im Zweifel — rufen Sie die Post direkt an: **0800 888 888** (gratis)
- Die echte Post-Website ist immer **post.ch**



Wenn Sie den QR-Code gescannt und bezahlt haben: Kontaktieren Sie sofort Ihre Bank und lassen Sie Ihre Karte sperren.

Nützliche Nummern und Ressourcen in der Schweiz

 Polizei (Notruf)

117

 Cyberkriminalität melden

cybercrime.ch

 Robinson-Liste (kein Telefonmarketing)

robinson.ch

 Bei Bankbetrug

Rufen Sie sofort Ihre Bank an

 Betrugswarnungen in der Schweiz

fedpol.admin.ch

Diesen Monat wird SeniorPhone unterstützt von:

[Platz für den Sponsor des Monats]

Nur ein Sponsor pro Monat — für Ihr Vertrauen.

Sécurité — À retenir absolument

 **Ne communiquez jamais vos mots de passe ou codes à qui que ce soit**

Ni par téléphone, ni par email, ni par SMS. Ni votre banque, ni la police, ni un opérateur ne vous les demanderont jamais.

 **Appel masqué — ne pas répondre**

Un numéro masqué cache volontairement son identité. Raccrochez sans hésiter.

 **Numéro inconnu — évitez de répondre**

Laissez sonner, attendez un message vocal, rappelez uniquement si nécessaire. Ne rappelez jamais un numéro 0900.

 **Faux policier ou faux banquier — raccrochez et appelez le 117**

La vraie police et votre banque ne vous demanderont JAMAIS de remettre de l'argent ou votre code PIN par téléphone.

Ce bandeau apparaît sur chaque fiche SeniorPhone — parce que votre sécurité est notre priorité absolue.

SeniorPhone — Einfache und ehrliche digitale Information für Senioren

 Um dieses Blatt per E-Mail zu erhalten: kostenlos anmelden auf seniorphone.ch

