INFO SHEET N°2

# Safety & Scams
# How to protect yourself?

*Scams often target seniors. This sheet helps you recognise them and protect yourself.*

*Every year in Switzerland, thousands of people are defrauded by phone, email or SMS. Seniors are particularly targeted — not because they are naive, but because scammers are very professional. Knowing their methods is already half the protection.*

## ⚠️ The most common scams

💻

### Fake tech support

🔴 **VERY COMMON IN SWITZERLAND**

You receive a call from someone claiming to be a technician from **Microsoft, Apple or Swisscom**. They tell you your computer is infected with a virus and they need remote access to fix it.

💬 *What they say: "Hello, I'm calling from Microsoft. We have detected a virus on your computer. I need to take control of your device to help you."*

✅ **Microsoft, Apple and Swisscom will NEVER call you spontaneously.** Hang up immediately. Never give a stranger access to your computer.

### 🏦 Fake bank employee

🟠 **RAPIDLY INCREASING**

Someone presents themselves as an employee of your bank and tells you your account has been hacked. They ask for your codes, passwords, or to transfer money to a "secure account".

💬 *What they say: "Hello, I'm from PostFinance. Your account is in danger. To protect it, I need your SMS code right now."*

✅ **Your bank will NEVER ask for your SMS code or password.** Hang up and call your bank directly using the number on the back of your card.

### 📦 Fake delivery SMS

🟡 **VERY FREQUENT VIA SMS AND EMAIL**

You receive an SMS or email saying a parcel is waiting for you and you must pay customs fees or click a link to confirm delivery.

💬 *What they write: "Your parcel N°CH8492 is waiting. Pay CHF 2.50 delivery fee here: [suspicious link]"*

✅ **Never click on a link received by SMS.** If you are expecting a parcel, go directly to the Post or DHL website by typing the address yourself.

### ❤️ Romance scam

🔴 **OFTEN VERY DIFFICULT TO DETECT**

Someone contacts you on social media or by email. They are charming, attentive, and claim to be falling in love. After a few weeks, they ask you for money for an emergency.

💬 *What they say: "I need to return from my mission as soon as possible to see you, but I need CHF 500 for the ticket. I will pay you back as soon as I arrive."*

✅ **Never transfer money to someone you have never met in person.** Talk to a trusted person before making any decision.

### 🎁 Fake prize / lottery

🟠 **CLASSIC BUT STILL EFFECTIVE**

You receive a message saying you have won a prize (car, holiday, sum of money). To receive it, you are asked to pay "administrative fees".

> 💬 *What they write: "Congratulations! You have been selected to win CHF 15,000. To receive your prize, please pay CHF 50 in processing fees."*

✅ **You never pay to receive a prize.** If you did not enter a competition, you cannot have won one. Ignore and delete.

## 🏆 SeniorPhone's 6 golden rules

1. **Never share your passwords or codes with anyone**

   Not by phone, not by email, not by SMS — never, to anyone, under any circumstances.

2. **Never click on a link received by SMS**

   Always type the website address yourself in your browser.

3. **If in doubt, hang up and call back yourself**

   Use the official number on the back of your bank card or on the official website.

4. **Never transfer money under pressure**

   Real financial emergencies can be verified. Take time to think and talk to someone you trust.

5. **Never give a stranger access to your computer**

   Microsoft, Apple and Swisscom never call you spontaneously to help you.

6. **Talk to someone you trust before acting**

   An outside perspective often helps spot a scam you may have missed.

## 📞 What to do with a suspicious call?

### 📵 Hidden number

Your screen shows *"Private number"* or *"Unknown"* — the person is deliberately hiding their identity.

**Do not answer. Hang up.**

### ❓ Unknown number

You do not recognise the number. Let it ring. If it is important, the person will leave a voicemail.

**Wait. Call back only if voicemail left.**

⚠️ **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.

### ✅ Key takeaways

→ Phone, SMS and email scams are very professional — it is not a matter of naivety.

→ Neither your bank, nor Microsoft, nor Swisscom will ever ask for your codes.

→ If in doubt: hang up, think, call someone you trust.

→ Never click on a link received by SMS, même s'il semble officiel.

→ You can report a scam to the cantonal police or at cybercrime.ch

# 📬 New scam — Fake Swiss Post delivery notice

## 🚨 Alert from the Geneva Cantonal Police — June 2026

Fraudsters are placing **fake delivery notices** in letterboxes that perfectly imitate those of Swiss Post. The document is extremely convincing and easy to mistake for the real thing.

### 📋 How the scam works:

1️⃣ You receive a fake Swiss Post delivery notice in your letterbox

2️⃣ It invites you to scan a QR code to "reschedule your delivery"

3️⃣ The QR code leads to a **fake website** that looks exactly like Swiss Post

4️⃣ You are asked for your details and a payment of CHF 2.10 in "fees"

5️⃣ **Real goal: steal your bank card details!**

### ✅ Essential rules to remember:

→ **Swiss Post NEVER asks for payment by QR code** for a delivery
→ **Never scan a QR code** received in your letterbox without checking
→ If in doubt — call Swiss Post directly: **0800 888 888** (free)
→ The real Post website is always **post.ch**

⚠️ **If you scanned the QR code and paid:** Contact your bank immediately to report the fraud and have your card blocked.

## 📞 Useful numbers and resources in Switzerland

| | |
|---|---|
| 🚔 Police (emergency) | **117** |
| 🌐 Report cybercrime | **cybercrime.ch** |
| 📋 Robinson list (stop cold calling) | **robinson.ch** |
| 🏦 In case of bank fraud | **Call your bank immediately** |
| 📰 Scam alerts in Switzerland | **fedpol.admin.ch** |



## 🔴 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.*