Worried about scam calls? Here's how to spot them and what to do in an emergency

By Steffen Zellfelder, Contributor, Tech Advisor JUN 12, 2025

They're not inevitable

Telephone fraud is widespread, and even prudent users can fall for the tricks of experienced scammers. Whether it's shock calls, the well-known but still successful grandchildren scam, or supposed calls from banks and authorities, the scams used by criminals are becoming increasingly sophisticated. They aim to exploit our fear, willingness to help or curiosity, combined with a lack of appropriate risk awareness.
The consequences are often serious, ranging from financial loss to considerable emotional stress. But there's also good news: if you remain alert, act cautiously and use modern technology in a targeted manner, you can protect yourself effectively against attempted fraud.
In this article, we'll show you how to recognise typical scams used by telephone fraudsters and what specific measures can help you protect yourself against calls to your mobile phone or landline.

Typical scams: What to expect at the moment

Fraud calls can look very different, but usually follow similar psychological patterns. Especially if you have older people in your family, it can be useful to talk to them about the topic and the typical tricks used by criminals so that they are forewarned.
Here are the most common scams at the time of writing:

The grandchild trick

This scam has been around for a long time, but unfortunately, it is still often successful.
Here's how it works. An alleged family member calls in tears or contacts you via WhatsApp with a new number (the old mobile phone has supposedly been stolen or lost).
The would-be family member then claims to be in an emergency – for example, after an accident – where money is urgently needed for an operation or for a lawyer.
The grandchild trick often targets senior citizens (hence the name) because they are assumed to be very helpful and technically naive.
Tip: Agree on a **code word** within your immediate family that only authorised family members know. This will allow you to clearly identify yourself on the phone if a dodgy call is made.

Fake police officers or bank employees

Fraudsters pretend to be employees of public authorities, such as the police or a bank. Alegedly, there has been a data theft or a burglary – now your money is at risk and needs to be secured urgently. Potential victims are then asked to hand over cash or make bank transfers.
Note: Real authorities or bank employees do not call to request money transfers or the return of valuables.

Technical support

The phone rings, and it's Microsoft – allegedly. The fraudsters also like to use Apple or other IT service providers as an excuse.
The scam: smartphones or computers are allegedly infected with malware, and you urgently need to carry out remote maintenance. As soon as you grant access, malware is installed, personal data is spied on, or your bank account is emptied.
Important: Reputable companies do not make unsolicited calls. Cancel such calls immediately.

Lottery prizes and fake competitions

You answer the phone and hear a voice: "Congratulations, you've won!". Well, that would be nice – but it's usually not true.
These callers first demand a "fee" for sending the prize or activating the winning account. You've probably already guessed it: The victims never see either the fee paid or the alleged prize again.

Ping calls

The phone only rings for a few seconds, and that's part of the scam. The aim is for you to call back out of curiosity.
The nasty surprise comes with the next mobile phone bill: the number often conceals an expensive international connection or a so-called "premium service" with high charges per minute. Sometimes, money is even automatically debited.
Typical dialling codes in such cases: 216 (Tunisia), 252 (Somalia), 387 (Bosnia). Note: These dialling codes can also change, so you should always be careful with unknown international calls.

Shock calls

You answer a call and suddenly a hysterical voice tells you about the alleged (and often serious) accident of a relative, an arrest or some other terrible catastrophe.
Once the scammers have successfully put the caller into a state of shock, money or other demands follow. The strategy: In a state of emotional emergency, victims are supposed to act rashly and allow themselves to be fleeced more easily.

Recognising warning signs – how to see through the scammers

If you recognise typical scams and listen carefully to dubious callers, you can effectively protect yourself from being ripped off, because most telephone scammers follow a similar pattern.
They rely on pressure, fear, stress or confusion. If you remain attentive, recognise typical warning signals and don't allow yourself to be pressured, you can often see through even sophisticated scams after just a few sentences. A healthy mistrust is the best protection here.
These are the typical characteristics of telephone scammers and their psychological tricks:

- **Emotional pressure/blackmail:** callers try to create fear, pressure or pity. Example: "I have no one else and I'm desperate, please help me!"
- **Threats**: "If you don't act immediately, I'll press charges!". Loss of money or damage to relatives can also be threatened.
- **High urgency:** Crooks rely on time pressure so that victims act as quickly and rashly as possible without being able to consult relatives or acquaintances.
- **Hidden numbers or foreign dialling codes:** Calls are often anonymous or come from a phone number of international origin.
- **Strange language:** Fraud calls are sometimes made using patchy language or a noticeable accent.

What to do in an emergency

Do you suspect you have a fraudster on the line? Here's how to react correctly:

- **Ask specific questions**: Fraudsters quickly become entangled in contradictions when confronted with specific questions. For example: "What is my grandson's full name?" or "Which office are you calling from exactly?".

- **Don't be rushed**: Serious callers will understand if you want to get a second opinion or continue the conversation later. If someone presses for an immediate or hasty decision, be very careful.
- **Speak out loud**: Simply state out loud what you are doing. For example: "I'm going to call the police now and sort this out". Crooks will then quickly end the call.
- **Hanging up is your right**: you don't have to justify yourself to anyone or listen to anyone on the phone. If something seems strange to you, hang up – it's better to hang up too soon than too late.
- **Check the phone number before calling back**: Use a search engine or online services such as Who called me? or Truecaller to check suspicious phone numbers.
- **Talk to acquaintances and especially older family members**: Older people in particular, are often not up-to-date on scams online or on their smartphones.

Technical protective measures: Get the hardware to help you

With the right settings and suitable hardware, you can make it harder for crooks to rip you off.

Improve scam protection on your smartphone

Activate call blocking: iOS and Android allow you to automatically filter unknown or blocked numbers. And this is how it works:

- **iOS:** Settings > Phone > Mute unknown callers
- **Android** (depending on the manufacturer): Phone app > Settings > Blocked numbers

Install caller recognition apps: These tools compare numbers with databases and warn of known scammers or their usual numbers. Popular apps include, for example:

- **Truecaller** (Android | iOS)
- **Clever Dialer** (Android | iOS)
- **Hiya** (Android | iOS)
- **Tellows** (Android)

Improve scam protection on your landline

With the right strategies and suitable devices, you can also build up an effective defence against scammers and fraudsters on landlines.

Use phones with a blocking function: Many modern DECT (Digital Enhanced Cordless Telecommunications) phones from Gigaset, Panasonic and other manufacturers offer block lists or even automatic blocking of calls with a suppressed number.

Set up a blacklist/whitelist: Some devices and routers allow you to specifically allow or block numbers.

See if your provider offers protection: Many phone service providers allow you to block certain calls via an app or online website.

What to do if you receive a suspected spam call

If you receive a suspicious call, always keep calm and preferably hang up immediately. Do not respond to questions or pressure, do not disclose any information and always be suspicious.

If you are unsure during the conversation, call the actual institution back yourself after hanging up – for example, your bank or the local police**. Very important: Always use the official number and** not the one left by the previous caller.

It is best to document the incident, i.e:

- Write down the phone number
- Note the content of the call
- If necessary, file a complaint with the police

You can also report suspected scam calls to the National Cyber Security Centre in the UK or the Federal Trade Commission in the US.

Tips for everyday life

These five simple rules will help you minimise the daily risk of scams and avoid falling for the sometimes very clever scammers:

- **Be economical with your contact details.** Especially with online competitions or on dubious/unknown websites.
- **Never call back.** If an unknown number only rings briefly, or if you have missed an international call that you cannot explain.
- **Talk to older family members.** They are particularly often the target of such scams.
- **Use a neutral answering machine.** If possible, do not give your full name in the greeting so that you give away less information.
- **Use an online service** to have private data deleted from the network.

If you know the common scams used by crooks, take warning signals seriously and use modern technology, you can recognise scam calls more easily and ward them off effectively. Our final tip: Stay vigilant and talk openly about the subject, especially with older people in your neighbourhood.

This article originally appeared on our sister publication PC-WELT and was translated and adapted from German.