THE BANK, THE POLICE, THE TAX OFFICE

Impersonation scam.

The fastest fraud there is. And the one move that ends it every time.

Hang up. Look it up. Call back.

This is an impersonation scam and it is the fastest fraud there is. A romance scam can run for weeks, months or years. This one can take twenty minutes. It does not need you to trust a person. It borrows the trust you already have in your bank, the police or a government office. And it runs on fear rather than hope.

> **Hang up. Wait five minutes. Call back on a number you looked up yourself. That single habit stops almost all of it.**

HOW IT USUALLY GOES

They already know things about you.

The call often starts with something correct. Your name. Your address. The last four digits of a card. A real payment you made last week. That information comes from data breaches, public records or an earlier scam. It proves nothing. It is there to make you stop doubting.

Then comes the problem. Your account has been accessed. A payment is going out now. There is a warrant in your name. You owe tax and officers are on their way. It is always urgent. It is always something only you can fix right now.

The number on your phone may show your bank's real name or number. That is easy to fake. Never treat the caller display as proof.

WHY IT WORKS

It borrows authority you already trust.

There is a name for this in psychology: authority bias. People comply faster and question less when an instruction appears to come from an authority. A uniform. A job title. A case number. A bank's name on the screen. The brain treats these as shortcuts and most of the time the shortcut is useful.

An impersonation scam rents that shortcut. The caller needs no relationship with you at all. They only need you to accept the role they are claiming. Then they add fear and a deadline, so there is no time left to test the role.

HOW AUTHORITY BIAS IS TRIGGERED

- **A name you already trust:** your bank, the police, the tax office, a well known company.
- **The props:** a case number, a badge number, a department, a reference you can write down.
- **Correct details about you:** your address or the last four digits of a card, offered as proof of office.
- **A number that looks right:** caller display can be set to any number, including your bank's real one.
- **Instructions rather than requests:** authority tells rather than asks. People follow.

Authority bias is normal and mostly useful. You need not become suspicious of everyone to be safe. One habit covers it: end the call and make contact yourself.

THE ASK

Always one of five things.

- Move your money to a “safe account” while they investigate.
- Read out a code that has just been sent to your phone.
- Install an app so they can “see the problem on your screen”.
- Pay a fine or a tax bill at once, often by transfer, gift cards or crypto.
- Help with a secret investigation. Tell nobody, not even staff in the branch.

What none of them will ever do

Your bank will never ask you to move money to another account to keep it safe.

Nobody legitimate will ever ask for your full password, your PIN or a one-time code.

The police will not take payment over the phone. They will not ask you to keep an investigation secret from your family or your bank.

A tax office will not demand immediate payment by gift cards, vouchers or crypto.

No real organisation will refuse to let you hang up and call them back.

THE SENTENCES, AND WHAT THEY MEAN

“Do not hang up, stay on the line while you do this.”

They need you to stay inside the pressure. Hanging up is the thing they fear most.

“If anyone in the branch asks, say it is for home improvements.”

They are coaching you past the one person who might stop this. Tell your bank the truth.

“We are testing our own staff, so this is confidential.”

Secrecy is never a security measure. It is the fraud protecting itself.

“You can check, this is the number on the back of your card.”

Caller display can be faked. Only a number you found yourself counts.

THE ONE MOVE

End the call, then wait.

1 **Say one sentence**

“I am going to call you back on the number I have.” Then hang up. You owe a caller nothing beyond that.

2 **Wait five minutes**

Better still, use a different phone. A caller can hold your line open and answer when you dial.

3 **Find the number yourself**

Look on your bank card, on your statement or on the official website. A number the caller gave you does not count.

4 **Then call**

If they were real, calling back costs nothing. If they were not, you have just ended it.

IF YOU HAVE ALREADY PAID OR SHARED SOMETHING

Start here, right now.

- Call your bank on a number you look up yourself. Ask them to stop or recall the payment.
- Change your passwords, starting with your email. Turn on two-factor authentication.
- If you installed anything, remove it. Have the device checked by somebody you trust.
- Keep the number, the messages and the times. Report it to the police and to your national fraud service.

> **Speed is their weapon. Slowing down is your defence. You are always allowed to slow down.**

People who lose money to an impersonation scam often say they knew about this kind of call. Knowing is one thing. Staying calm while a stranger tells you your savings are disappearing is another. This was done to you on purpose, by somebody trained to do it.