



THE BOOK OF PHONE SCAMS



230924CD

Working in partnership, making communities safer
www.westmidlands.police.uk

Introduction

1/3

Nearly a third of all fraud is committed over the telephone.

National Fraud Intelligence Bureau

Criminals are experts at impersonating people or organisations (like banks, the tax office or even the police).

They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.



Stop:

Taking a moment to stop and think before parting with your money or information could keep you safe.



Challenge:

Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.



Protect:

Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

FRAUDSTER'S TACTICS

###

Criminals can disguise their phone number to make it look like anyone they want.



They can call you with what looks like a genuine phone number, either using a computer or human voice.



They will keep your landline open by not hanging up and even play a dialling tone over the phone.



They can send text messages requesting you call them, click on a link, or enter a One Time Password (OTP). **These scam messages can appear alongside your genuine messages.**



And send website links which can steal your data and money when you click on them.

**Don't trust the Caller ID display on your phone,
a phone number is not proof of ID.**

You are called by...

a computer or phone company

THE CLAIM

You have a problem with your computer.

Criminals may call and claim that there are problems with your account, computer or Internet. They claim to be your computer manufacturer, telephone, internet or streaming service provider, or an online shopping platform and suggest they can help you.

THE SCAM

They instruct you to download a program which gives the criminal remote access to your computer.

They can then access your passwords, photos, data and even your bank account if you log in to it.

PROTECT YOURSELF



If you receive a call like this **hang up**.
'Take Five' and **verify** via a trusted method,
not via numbers given in the call.



Never allow **anyone** to remotely access your
computer.



Do not download software on the request
of a phone caller.



A genuine service provider will **never** call you
out of the blue regarding issues with your
computer.



If you are having problems with your internet
connection, **contact your internet provider**
on a number or email address that you **know**
to be genuine.

You are called by...

your bank or the tax office

THE CLAIM

There is an issue with your account.

Criminals may call and claim to be from your bank and allege there is a problem with your account.

Or they claim to be from the tax office and declare a warrant is out for your arrest.

THE SCAM

They instruct you to pay money into a “secure account” they control to “keep it safe”. Or, they get you to type in personal details, including One Time Passwords (OTPs) and gain access to your account. Or they tell you to pay a fine to avoid arrest.

All of these are scams!

PROTECT YOURSELF



If you receive a call like this **hang up**.
'Take Five' and **verify** via a trusted method,
not via numbers given in the call.



The bank scam normally follows a scam
email, so they may know who you bank with
or even how much money is in your account!



Your bank will **never** ask you to transfer
or withdraw money. Or set up a “secure
account” for you.



The tax office do **not** threaten arrest or
request payment of fines over the phone.



Seek advice or a second opinion; speak to
friends or family if you are unsure. A genuine
caller won't mind you checking.



Never share your PIN, password or OTP with
anyone, especially if they initiated contact.
Not even by tapping in into your phone.

You are called by...

the police

THE CLAIM

We need your help with an investigation!

Criminals impersonate the police, and often state there are corrupt staff at your bank, or criminals have cloned your bank cards and request your assistance with the investigation.

THE SCAM

They instruct you to provide your bank cards and PINs, or withdraw money, purchase high value goods (like watches) or vouchers and hand these over to a courier or “undercover officer” as evidence.

The “Undercover officer” is a criminal or the courier delivers your cash, cards and purchased items to the criminals.

PROTECT YOURSELF



If you receive a call like this **hang up**.
'Take Five' and **verify** via a trusted method (like calling 101), not via numbers given in the call.



The police will **never** ask you to participate in an undercover investigation.



The police will **never** ask you to transfer or withdraw money or buy items on their behalf or for evidence.



The police will **never** attend your home to collect your cash, bank cards or ask for your pin.



Speak to friends or family if you are unsure. A genuine officer won't mind you seeking advice or double checking.



Never share your PIN with **anyone**. Not even by tapping it into the keypad on your phone.

Reporting Scams

- Contact your bank immediately if you think you've fallen for a scam and report it to **Action Fraud**; either online at **www.actionfraud.police.uk** or by telephone on **0300 123 2040**.
- Every report **assists** police investigations, **provides** intelligence, **informs** national alerts that protect all communities, **disrupts** criminals and **reduces** harm.
- Contact police directly on **101** or **999** in an emergency.
- Forward any scam text messages to **Ofcom** on **7726** (free of charge).
- All major phone companies provide a **call blocker service**. This should help screen out most phone scams shown in this booklet. Contact your telephone service provider to find out more.

5 THINGS TO LOOK OUT FOR ON A SCAM PHONE CALL

- 1.** The caller doesn't give you time to think, tries to stop you speaking to a family member or friend or is insistent and makes you feel uncomfortable.
- 2.** The caller asks you to transfer money to a new account.
- 3.** The caller asks for your 4-digit card PIN, passcodes, One Time Passwords (OTP's), or your online banking password. Even if they ask you to give it to them by tapping into the telephone keypad rather than saying the numbers out loud, this is a scam.
- 4.** The caller asks you to withdraw money to hand over to them for safe-keeping.
- 5.** The caller says that you are a victim of fraud and offer to send a courier to your home to collect your cash, PIN, payment card or cheque book.

For more information please visit
<https://takefive-stopfraud.org.uk>



THE BOOK OF PHONE SCAMS



230924CD

Working in partnership, making communities safer
www.westmidlands.police.uk