

# THE LITTLE BOOKLET OF PHONE SCAMS



Eastern Region Special Operations Unit



Regional Organised Crime Unit

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

National Fraud Intelligence Bureau

**Criminals can impersonate your bank, the police, tax office, investment or software companies and other trusted organisations. They will try to convince you to part with your money.**

**Hang up on cold calls from any business/authority, then 'Take Five' to check it out as genuine via a trusted source.**

**The three most common scams are:**

1. Your computer has a problem
2. A fraud investigation
3. An investment opportunity

## Fraudster's tactics

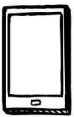
Criminals can disguise their phone number to make it look like it's from a bank, the tax office, the police... or anyone.



They can call you with what looks like a genuine phone number.



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



They can text messages requesting you call them, or click on a link.

**These messages usually appear in the same text thread as genuine messages.**



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

**Never trust the caller ID display on your phone, it lies to you!**

# SCAM 1 A COMPUTER PROBLEM

## THE CLAIM

### **You have a problem with your computer.**

Criminals may call and claim that there are problems with your computer or internet. They claim to be your computer manufacturer, telephone or internet service provider 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 bank details, data and passwords.



## 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 issues with your computer, **contact the retailer** you purchased it from.
-  If you are having problems with your internet connection, **contact your internet provider**.

## THE CLAIM

**Your bank account has been compromised.**

Criminals may call and claim to be from your bank, the tax office or police and claim there is a problem with your bank account.

They 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 transfer money into a secure account, provide cash, high value goods (like watches) or vouchers to a courier.

They tell you the account is in your name but in fact it **belongs to the criminal!** and 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,  
not via numbers given in the call.
-  Your bank, the tax office or the police  
will **never** ask you to transfer or withdraw  
money or buy items on their behalf.
-  Your bank, the tax office or 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.
-  **Never** share your PIN with **anyone**.  
Not even by tapping it into the keypad  
on your phone.

## SCAM 3 AN INVESTMENT OPPORTUNITY

### THE CLAIM

#### **We have an investment opportunity for you!**

Criminals may call you to persuade you to invest in all kinds of products, including diamonds, wine or art.

They offer low risk and high rates of return, claiming it's a once in a lifetime opportunity and you'll have to act quickly.

### THE SCAM


If you do invest, the criminals will often request further 'transport' and 'storage' costs.

**These investments do not exist.**





## 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.
-  Genuine investment companies will **not** cold call you.
-  Don't be pressured into making a quick decision and seek **impartial** financial advice before committing to any investment.
-  There are no 'get rich quick' schemes. **If it sounds too good to be true, it probably is.**
-  When investing with genuine companies research what you have been offered and the investment company. Speak to the **Financial Conduct Authority** if you have concerns. Call **0800 111 6768** or visit **www.fca.org.uk**

**Always** report scams and fraud to Action Fraud, either online at **[www.actionfraud.police.uk](http://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).

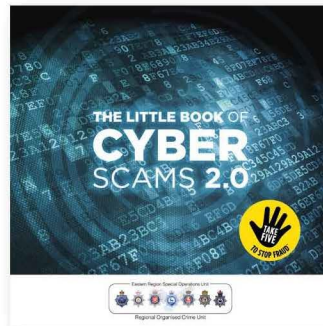
All major phone companies provide a **call blocker service**. This should help screen out most phone scams shown in this booklet. Contact your telephone service provider to find out more.

Don't assume others in your life know the information you've read here. Tell2 friends and family and together we can protect many.

To contact the Eastern Region Cyber Crime Unit  
email [cyberprotect@ersou.pnn.police.uk](mailto:cyberprotect@ersou.pnn.police.uk)  
or call **01707 355464**.

For more information visit  
<https://ersou.police.uk>

For more literature and videos visit  
<https://www.met.police.uk/littlemedia>



# **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.** They phone to ask for your 4-digit card PIN 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.** They ask you to withdraw money to hand over to them for safe-keeping.
- 5.** They may say 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/advice/>**