Computer Misuse Act

Contents

1 Introduction

In this document we explain briefly *what* is, *why* we have it and what are the main core principles that are essentially used, during an investigation, to establish whether a person accused of *computer misusing* is actually guilty of an offence or not

1.1 What it is

The Computer Misuse Act protects personal data held by organisations from unauthorised access and modification like entering a computer system without permission (hacking) and maybe even with intent to commit a further crime (which increases the penalty)

1.2 Why we have it

To make sure confidential data doesn't get shared by people with criminal intent

2 The key principles

These principles are a kind of tickbox list. If any one of these boxes ticks, then, one can be considered liable and guilty for committing an offence.

2.1 1st principle

The first principle that needs to be verified to establish whether a person is guilty of an offence is : having evidences of unauthorized access to computer material.

2.2 2nd principle

It's like the 1st principle but in this one we also have the intent to do it on purpose which increases the penalty. The exemption applies to an officer carrying out of powers of investigation, powers of search and seizure or any other investigatory powers granted by statute, but if you're not an officer you're essentially looking for troubles.

2.3 3rd principle

It's like the 2nd principle adding the intent to facilitate futher offences which increases the penalty even more for a maximum of 14 years or life-time imprisonment. The only exemtpion once again applies if you're a police officer,an officer of the Serious Fraud Office, you're working for the National Crime Agency or naturally HM Revenue and Customs.