

**Review of the Computer Misuse Act 1990**

Consultation and Response to the Call for Information

This consultation begins on 7 February 2023

This consultation ends on 6 April 2023

**About this consultation:**

|  |  |
| --- | --- |
| **To:** | This is a public consultation which may be of particular interest to:   * Law Enforcement Agencies * Domain name registrars and registries * Hosting providers |
| **Duration:** | From 07/02/2023 to 06/04/2023 |
| **Enquiries to:** | Cyber Policy Unit  Homeland Security Group  Home Office  5th Floor, Peel Building  2 Marsham Street  London  SW1P 4DF |
| **How to respond:** | Please provide your response by 6 April 2023 to [cmareview@homeoffice.gov.uk](mailto:cmareview@homeoffice.gov.uk)  We would be grateful for answers to the specific questions included throughout this document.  Please also use the contact details above if you require information in any other format, such as Braille, audio or another language.  We cannot analyse responses not submitted to the email address set out above. |

# Contents

[Contents 2](#_Toc126303542)

[Ministerial Foreword 3](#_Toc126303543)

[Background 5](#_Toc126303544)

[Review of the Computer Misuse Act 1990 6](#_Toc126303545)

[Proposals for Legislative Change 8](#_Toc126303546)

[Domain name and IP address takedown and seizure 8](#_Toc126303547)

[Power to preserve data 12](#_Toc126303548)

[Data copying 13](#_Toc126303549)

[Areas for further consideration 15](#_Toc126303550)

[Introduction 15](#_Toc126303551)

[Extra-territorial provisions 15](#_Toc126303552)

[Defences 15](#_Toc126303553)

[Sentencing 16](#_Toc126303554)

[Glossary of Key Terms 18](#_Toc126303555)

# Ministerial Foreword

Cyber crime threatens our citizens, businesses and government. State actors and criminals, at all levels of complexity and with varying intent are targeting homes and businesses across the UK. As Security Minister, it is my responsibility to ensure that we have the right legislative framework, powers and law enforcement capability to tackle this threat.

We have already taken significant steps to provide our law enforcement agencies with the skills and resources they need to be able to investigate and prevent criminals from attacking us. The National Cyber Fund has boosted investment, increased capability and expanded training to improve the law enforcement response. The National Cyber Crime Unit (part of the NCA) has brought together law enforcement experts into a single elite unit. We have established a network of Regional Organised Crime Units (ROCUs) which include cyber crime units, to provide access to specialist capabilities at a regional level to forces. The law enforcement response to cyber crime across England and Wales has changed so that it operates as one nationally networked resource, able to react to any given situation and based on the best available intelligence.

To ensure that the UK’s legislative framework continues to support action against the harms caused by criminals operating online, the Government has carried out a review of the Computer Misuse Act 1990 (CMA / the Act). We held a Call for Information on the CMA and the powers law enforcement agencies need to investigate the CMA offences, and a number of proposals were put forward, both for changes to the Act itself, and for additional powers to allow law enforcement agencies to more effectively tackle the offences covered by the Act.

This consultation now seeks your views on three proposals for legislation. The first relates to the proposal for the development of a new power to allow law enforcement agencies to take control of domains and internet protocol (IP) addresses where these are being used by criminals to support a wide range of criminality, including fraud and computer misuse. We recognise that a significant amount is done under voluntary arrangements to tackle the misuse of domain names, and we would not want to see these arrangements undermined, but I believe that we need to ensure that where such arrangements are unavailable, law enforcement agencies have the power to take action.

The second proposal is for a power to allow a law enforcement agency to require the preservation of computer data in order to allow that law enforcement agency to determine whether the data would be needed in an investigation. The power would not allow the law enforcement agency to seize the data, but would allow it to be preserved in case needed.

Finally, we would welcome views on whether a power should be created that would allow action to be taken against a person possessing or using data obtained by another person through a CMA offence, such as through accessing a computer system to obtain personal data, subject to appropriate safeguards being in place.

This document also contains details of our proposed approach to a number of other issues which were raised during the review. These included proposals on the levels of sentencing, defences to the CMA offences, improvements to the ability to report vulnerabilities, and whether the UK has sufficient legislation to cover extra-territorial threats. These are complex issues, and therefore the Home Office will lead a programme to bring stakeholders together to identify how these issues should be addressed to ensure that the UK’s cybersecurity can counter the risks posed by state threats and criminals.

**Rt Hon Tom Tugendhat MBE VR MP**

**Security Minister**

# Background

A wide range of hostile actors use cyber capabilities to target the UK. They include foreign states, criminals, "hacktivist" groups and terrorists, and the threat posed by cyber attacks continues to grow in scale and complexity. In the year ending March 2022, there were an estimated 1.6 million (1,633,000) incidents of computer misuse experienced by adults aged 18 and over in England and Wales, of which 335,000 (21%) were computer virus related and 1,298,000 (79%) were related to unauthorised access to personal information (including hacking). Computer misuse accounted for 14% of overall crime in this period.

[The National Cyber Strategy 2022](https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022) signals a shift to a more comprehensive national cyber approach, drawing together our capabilities inside and outside government. The strategy will be guided by the 5 pillars on strengthening our cyber ecosystem, building resilience, investing in technology, advancing global leadership, and disrupting our adversaries in cyberspace.

[The Integrated Review of Security, Defence, Development and Foreign Aid](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf) highlights the importance of strengthening the defence against state threats.

# Review of the Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) is the main legislation that criminalises unauthorised access to computer systems and data, and the damaging or destroying of these. The Act has the intention of protecting the integrity and security of computer systems and data through criminalising access to them which has not been authorised by the owner of the system or data.

In May 2021, the Home Secretary announced a review of the CMA. The first step in the review was a public Call for Information seeking the views of stakeholders and the wider public, to identify and understand whether there is activity causing harm in the area covered by the CMA that is not adequately addressed by the current offences. The scope included whether law enforcement agencies have the necessary powers to investigate and take action against those attacking computer systems, and whether the legislation is fit for use following the technological advances since the CMA was introduced.

Responses were received from 51 stakeholders and covered a range of proposals where respondents felt more could be done to protect the UK and take action against criminals. These included:

* New powers for law enforcement agencies to allow them to investigate CMA offences more effectively
* Ensure that the UK can take action against offences committed extra-territorially or that affect the UK when committed overseas
* Statutory defences to the CMA offences
* Ensuring that sentencing levels are appropriate
* Offence of possession of illegally obtained data
* Improved training for the judiciary and prosecutors
* Consideration of whether new technologies, such as AI and the internet of things, are adequately covered under the CMA
* Failure to prevent cybercrime / duty to protect
* Online harms, such as deep fake imagery

Some of these proposals, such as online harms[[1]](#footnote-2) and the cyber duty to protect[[2]](#footnote-3), are being considered under other programmes.

Following the Call for Information, it is clear that much of the CMA remains effective in allowing law enforcement agencies to take action against those committing the harms covered by the Act. Prosecutors and the courts have been able to use the Act to prosecute and convict those who commit the offences, in spite of the significant changes in technology since the Act was introduced, reflecting the technology-neutral nature of the legislation.

However, the Call for Information raised a number of important issues in relation to specific areas of the Act, and to the powers available to law enforcement agencies to investigate these offences. This paper sets out the Government’s response to these proposals, with the aim of ensuring that our response keeps pace with the threat.

There are two areas of work that we will undertake. Firstly, there are a number of proposals for change that we believe are sufficiently clear for us to consult on with a view to legislating when Parliamentary time allows. These form the first section of this paper.

The second section sets out the approach we will take to a number of other areas where we believe that more work needs to be done to identify what action should be taken. We are proposing that this is done through a multi-stakeholder approach, led by the Home Office.

# Proposals for Legislative Change

## Domain name and IP address takedown and seizure

**Context**

Criminals use domain names and IP addresses to support a wide range of criminality, including offences such as the distribution and control of malicious software (“malware”), phishing, fraud, and the sale of illegal goods such as drugs or firearms.

These cause substantial harm to the UK’s citizens and businesses. There is already significant work to tackle these websites and remove them, such as that led by Action Fraud and the National Cyber Security Centre (NCSC), on a voluntary basis. We would expect these arrangements to continue, and the firm intention is that these should remain the primary means of taking down domains that are supporting criminal activity as they provide a fast and effective response.

However, while these voluntary arrangements are often effective, some stakeholders have suggested that these are not available in all circumstances, and that a formal power is necessary where such arrangements are not available or usable.

Such powers exist in the United States and elsewhere across the globe, and having such powers would allow the UK to work effectively with overseas law enforcement agencies to tackle a global problem.

We therefore believe that as there is no specific power available to law enforcement agencies, given the key role that criminal misuse of domains has in many types of crime, we need to consider whether there should be powers available to enhance our ability for law enforcement agencies to take a range of actions against these threats.

**Take down**

One of the simplest ways of dealing with the criminal use of domain names is to require the registrar responsible for the creation of the domain name to remove it from the list of registered domains. This will prevent anyone from accessing the website, and prevent criminals from misusing it. The power would also apply to seizing IP addresses as criminals can (and do) on occasions just use IP addresses in their malware.

**Takeover by law enforcement**

Domain names are used by criminals to link their command-and-control platforms with infected computer systems to control them. In some cases, industry takedowns can be insufficient to stop these background processes from continuing to operate – mitigating the harm therefore requires administrative command of the domains or IP addresses themselves to be taken quickly, and at scale.

A prime example of the application of domain control relates to tackling botnets. A botnet is a network of infected systems, typically being controlled without the knowledge of victims, whose computers are being controlled as a platform to further promulgate malicious activity (e.g. sending spam, acquiring data, proxying criminal communications or carrying out denial of service attacks). Such botnets can operate at significant scale: in one current case alone, an estimated 1.5 million systems worldwide have been infected with malware. In other cases, botnets have been used to generate hundreds of millions of dollars of losses from victims’ systems globally. The ability of law enforcement agencies to seize domains and/or IP addresses is already available in most developed jurisdictions, but is not available to UK law enforcement. Were a power to be available here, it would enable domestic law enforcement to break the communication link between criminal and victim computers.

Once law enforcement have taken control of the domains or IP addresses other possibilities also become available to them. For example, they could choose to “sinkhole” (see [**glossary of key terms**](file:///C:\Users\millarj4\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\6IKX2IRW\DN_Takedown_JM-SG_Tracked_edits.docx#_Glossary_of_Key)) the incoming victim communication attempts. This “sinkholed” data can be used to identify how many victims there are, what IP address they are on, and on occasions further details about the infected device – such as its operating system, which can help defenders find it and clean it. Sinkholed data can be disseminated through existing channels to notify victims around the globe that they may be infected.

We believe that the UK would benefit from law enforcement agencies being given the right to cede control of the domain and/or IP addresses to trusted parties for management and sinkholing efforts, to remove the need for law enforcement agencies to renew millions of domain names every year to ensure they do not fall back into criminal hands. There are existing trusted non-profit organisations that could undertake this function without adding cost to the public purse, whilst simultaneously improving feeds to national cyber security incident response teams (CSIRT), including the UK’s National Cyber Security Centre (NCSC).

**Prevent domain name creation**

There are cases where it is possible to predict that certain domain names will be created for criminal purposes, perhaps to mimic a business or a government department, for the purpose of committing fraud. We believe that there would be benefits to requiring the UK Registry not to register defined domain names to prevent such fraud or other criminal activity.

There are cases where it is possible to predict that certain domain names will be created for criminal purposes as the malware on infected devices uses an algorithm to determine what domain(s) it will try and connect to. These Domain Generation Algorithms (DGAs) give criminals an asymmetric advantage – since criminals only have to control one domain each day – whilst law enforcement may have to control hundreds or thousands of possibilities each day. DGAs are predictable and so it is possible to predict what domains will be viable on any given date. We believe that there would be benefits to requiring the UK Registry not to register such predicted defined domain names to prevent such criminal activity. The ability to legally do this in the UK would make it possible to make similar requests of law enforcement in other countries where the majority of registries are located, particularly as some will not act in response to law enforcement requests unless they are accompanied by a court order.

**Use of the power**

A request to take down, seize or prevent the creation of a domain name would be served on the relevant party who was in control of the domain, such as the Registry (who create it and ensure that only one instance of it exists), a Registrar (who effectively leases it) or the Registrant (who rents it and deploys their content).

A request to seize control of an IP address would be served on a network provider that controls that IP address. They might be required it to tunnel that IP to another in the control of law enforcement or other trusted party.

We propose that this power is available to specified public authorities, and would welcome views on which agencies should be able to use it.

As cyber attacks often span multiple jurisdictions, we therefore propose that this power is available for use in response to a request from overseas under mutual legal assistance, or emergency requests. This would allow law enforcement agencies to require the takedown of domain names, both for domestic investigations and as part of joint investigations with overseas partners.

We propose that law enforcement agencies would need to apply to a court for the order, and would need to demonstrate evidence that the domain was supporting criminality (or can be shown will potentially support criminality where its generation can be predicted) and that the suspension of the domain would reduce or remove that threat or otherwise significantly support an investigation.

The person required to carry out the action should have the right to appeal to the court to remove the suspension, as should the registrant where domain names have been registered. However, the suspension should remain in place while the appeal is taking place and refusal of the request by the person on whom it is served will result in a fine.

Finally, there should be a route for registrants to apply for compensation should be made available if they believe the domain or IP address they lease has been wrongfully seized. The liability for the action lies with the law enforcement agency.

Questions

Q1. What should be the threshold for the use of this power, what tests would an application have to meet and what safeguards should apply to it?

Q2. Which organisations should have access to the power?

Q3. What will a statutory power enabling the seizure of domain name and IP addresses allow that voluntary arrangements do not currently allow?

Q4. What activity would we ask the recipients of an order to undertake that they do not undertake under voluntary arrangements?

Q5. How can voluntary agreements, which are the preferred route for take downs, be protected?

Q6. Should seizure mean the legal control and ownership (at least of the lease period) of domain names and IP addresses, or more temporary action such as sinkholing, pass to the law enforcement agency responsible for the order? Would law enforcement agencies pay for the lease?

Q7. If action is taken by law enforcement, should that be done for both the domain name and the IP address, and are there different recipients for orders for these?

Q8. Should multiple domains / IP addresses feature on one application or will separate applications be required?

Q9. Should there be scope for an emergency interim order to be made in advance of a hearing for a full order?

Q10. Should there be an opportunity for extensions to the order?

## Power to preserve data

**Context**

There are very few offences where it would not be conceivable that electronic evidence could be required as part of an investigation, and it is therefore essential that law enforcement agencies are able to require the preservation of existing data by a data owner to prevent that data being deleted. Preservation would require the data to be retained by the system owner in an unaltered state, pending a decision on whether a formal request for seizure of the data by a law enforcement agency should be made to a court.

This proposal does not apply to information where the retention of data is already required, such as that under the Investigatory Powers Act 2016.

Data is preserved voluntarily at the request of law enforcement agencies, and this process works well. However, given the need for electronic evidence to be available for investigations in an increasing number of cases, we believe that it is necessary for the UK’s law enforcement agencies to have access to a power that requires the preservation of data where a person is unwilling to do so voluntarily.

**Proposal**

We propose that there should be a power enabling law enforcement agencies to require the preservation of specified computer data by a person in control of such data. This power would not permit a law enforcement agency to seize data, but is intended to allow time for an agency to determine whether the data is relevant to an investigation. If the data is required, the necessary authorisation would need to be obtained under existing legislation, such as the Police and Criminal Evidence Act 1984, from a court to seize the data. This power would apply to any data relating to any offence.

Given the wide range of offences where electronic data might be needed during an investigation, we propose that this power should be available to all UK law enforcement agencies, including the National Crime Agency (NCA), UK police forces, HM Revenue & Customs (HMRC), and the Serious Fraud Office, and other departments and agencies responsible for tackling crime.

We also propose that the power should be available for a law enforcement agency to use in relation to a request from an overseas law enforcement agency, subject to the UK’s existing safeguards for international cooperation.

As this is a power that does not involve data being obtained by the agency requesting its preservation, we propose that this power must be signed off by a senior officer for the organisation.

The data owner should have the right to appeal to a court against the requirement to preserve the data in question. However, the data should be retained while the appeal is taking place and action to delete, alter, or prevent access to the data will result in a fine.

To prevent any significant cost burden being placed on business, the power must have a set timeframe for preservation, after which the data owner is free from the requirement to preserve the data. The Budapest Convention on Cybercrime provides for a time limit of ninety days, and we believe that this would be reasonable timeframe.

Questions

Q1. Which agencies should be able to use this power?

Q2. Are there any problems associated with preserving data that we need to consider?

Q3. Should there be a time limit on the preservation order? If so, what should that be?

Q4. Who should be responsible for covering any costs of preservation? How should they be determined?

Q5. Are the existing powers in the Police and Criminal Evidence Act 1984 Schedule 1 already sufficient to allow preservation?

## Data copying

**Context**

The CMA covers unauthorised access to computer data but the unauthorised taking or copying of data is not covered by the Theft Act and this is established in case law. The simple copying of data would only attract the penalties under section 1 of the Computer Misuse Act of a fine and / or up to two years maximum imprisonment. This could be considered an insufficient penalty to deal with the seriousness of the criminality.

Section 2 could be used to prosecute those who, for example, copy data in order to perpetrate fraud, which carries a maximum sentence of up to five years imprisonment.

There is a long-running concern relating to the difficulty of taking action against a person possessing or using data obtained through a CMA offence, such as where the person who holds the data did not commit the CMA offence. It is not possible to charge that person with theft or handling stolen property, as theft is defined in the Theft Act as “permanently depriving”, whereas most theft from computer systems involves copying the data. There are provisions in the Fraud Act that allow the prosecution of those using such data to commit fraud offences[[3]](#footnote-4).

**Proposal**

We would like to consider whether there is a need to create a general offence for possessing or using illegally obtained data, and would welcome views on the necessity.

Questions

Q1. What is the gap in current legislation, and what effect does that have?

Q2. Are there examples of where harm is caused by the absence of an offence?

Q3. What is the appropriate penalty if such an offence was created?

# Areas for further consideration

## Introduction

There were number of areas raised during the review that the Government believes need further consideration, and we propose that a multi-stakeholder programme, to include prosecutors, investigators, other government departments and the cybersecurity industry, should be set up to consider them.

## Extra-territorial provisions

The nature of CMA offences is such that they cut across international jurisdictions. Individuals can be acting in any country or routing their software through different host countries; so that the offending is not necessarily taking place in England and Wales; whereas the victim may be. While the jurisdiction in CMA cases is further reaching than other legislation, there remain grey areas. For instance, the definition of “significant links” can be open to different interpretations. Stakeholders have proposed that it would be simpler if there were one clear definition of “significant link” that applied across the whole of the CMA (currently this differs between sections).

Stakeholders have also suggested that we explore how we could gain the ability to prosecute for all aspects of a cyber criminal activity in the UK, rather than restricting such a prosecution to conduct where there is asignificant link. This would be particularly important where such an individual may seek to locate themselves in a jurisdiction that cannot or will not investigate and prosecute. Many jurisdictions lack the investigative ability or the legislative tools necessary to prosecute extra territorial criminality.

## Defences

One of the main issues raised during the review of the CMA was that regarding whether statutory defences should be introduced to the offences in the Act for those taking action to protect the UK in cyberspace. The arguments put forward were that the Act potentially criminalises what many in the cyber ecosystem regard as legitimate cyber security activity, and that it inhibits the growth of the industry itself.

The Government has carefully considered this proposal, and we believe further work is required to consider options, and the risks and benefits associated with the introduction of statutory defences. The Act is based on the principle that access to computer systems and data must be authorised by those with responsibility for them.  As the Government is encouraging system owners to do more to protect their systems, including through employing legitimate cyber security companies to test their security, it is right that we continue to protect the system owners from those who access, or attempt to access, their systems without their agreement. Alongside that, we must be able to take action against criminals and state actors who threaten the UK in cyberspace, and not make changes that would provide cover for criminal activity. Finally, we need to make sure that any defence does not provide cover for offensive cyber activity, sometimes known as “hack back”.

We must also consider the benefits that the introduction of defences could provide. A strong cyber ecosystem is central to the UK becoming a more cyber secure and resilient nation, better prepared for evolving threats and risks, adopting good cyber security practises. We therefore need to ensure that the cyber security industry is not unnecessarily prohibited from conducting activities that would protect entities and individuals from hostile cyber actors – activities that would advance our whole of society approach to cyber security – while respecting the principle that access to computer systems and data must be authorised by those with responsibility for them.

In the National Cyber Strategy, the Government has set out its aim of enhancing the UK’s cyber security, and the Government believes that we need to consider whether and what defences, including both legislative and non-legislative solutions, should be introduced in the context of how the cyber security industry can be supported and developed to help protect the UK in cyberspace.  As part of that work we need to consider what activity that may conflict with the CMA is legitimate for cyber security companies to undertake, and what standards and training cyber security professionals must have in order to be qualified to undertake such activity.  We will take this work forward as part of the wider work to improve our national cyber security.

## Sentencing

A number of questions were raised as part of the review relating to sentencing, and in particular whether the sentence levels are appropriate for the harms caused by the offences in the CMA. The section 1 CMA offence of unauthorised access to computer material carries a maximum penalty of up to 12 months in prison on a summary conviction, or two years on indictment, or a fine or both. Some stakeholders suggest that this does not deter criminals and does not reflect the seriousness of the offending, however sentencing data (December 2021)[[4]](#footnote-5) shows that courts are not currently issuing sentences near to the maximum under the Act. Therefore, we need to consider whether increasing sentence lengths would impact the severity of penalties issued for CMA offences.

Stakeholders have also proposed that sentencing guidelines would be an appropriate way forward to address the following issues:

* Cutting across the wide spectrum of offences included in the CMA, from children experimenting on the internet through to hostile state actors.
* Many CMA cases have a neuro-diversity element attached to the offender, making the individual(s) concerned more vulnerable and therefore more difficult to prosecute with proportionate sentences.
* The CPS highlighted that (applying the Code for Crown Prosecutors) they charge offenders using the most appropriate offences to reflect the nature of the offending, the extent of the criminality and those offences that can best be presented to the courts and juries. There are already sentencing guidelines in relation to fraud and money-laundering and as result, building up a picture in court is more straight-forward to assist the Court in the sentencing procedure. The lack of such guidelines in CMA cases can lead to inconsistences in the approach to the harm of such offending.

# Glossary of Key Terms

Sinkholing

Sinkholing is a technique for manipulating data flow in a network. It involves redirecting traffic from its intended destination (in this context – one set by the criminal) to another server of your choosing. This server can be configured to log the incoming communication’s IP addresses, date/time stamps and other information which might identify the individual infected device more precisely but does not log any criminally exfiltrated data. Security professionals commonly use sinkholing as a tool for research and reacting to attacks.

Sinkholing can refer to both *sample sinkholing* and *full sinkholing*. *Sample sinkholing* registers a single domain known to be checked by malware and logs the IP addresses of victim devices trying to contact it. *Full sinkholing* allows for all the domains malware tries to connect to each day to be sinkholed. This has a two-fold effect - generating victim IP lists that can be used to notify victims via existing channels, and protecting the victims from exploitation.

Domain name

A domain name is the name of a website and typically consists of a top-level and second-level domain. A top-level domain (TLD) is the part of the domain name located to the right of the last dot, with the most common TLDs being .com, .org or a country name such as .uk. A second-level domain (SLD) is the part of the domain name located to the left of the last dot, such as gov.uk.

It is possible for a domain to resolve to multiple IP addresses, and it is also possible for multiple domains to resolve to the same IP address. The latter is often used by large hosting providers. IP addresses can be traced through existing processes to identify who is providing them and where in the world they are located and offer a first step in identifying who legitimately controls the IP address, and who might be criminally controlling it.

Domain names are created and leased by authorised registrars (e.g. GoDaddy (US)) and issued by registries e.g. Nominet for .uk domains. Working together, Registries and Registrars ensure that the name is not already registered. When a new .uk domain name is created, along with its IP address, the details will be sent by the Registrar to the relevant Registry (Nominet), and those details are held on the global WHOIS database.

When a registrant purchases the right to lease a domain name they only typically deal with Registrars, of which there are many globally, each making available a variety of possible TLD’s and dealing with one or more Registries.

1. [Online Safety Bill: factsheet - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet) [↑](#footnote-ref-2)
2. [Call for information: Unauthorised access to online accounts and personal data - GOV.UK (www.gov.uk)](https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data#about-this-call-for-information) [↑](#footnote-ref-3)
3. Fraud Act 2006, s6 [↑](#footnote-ref-4)
4. [↑](#footnote-ref-5)