TransUnion

# The Transunion Fraud Education Handbook for Students

Fraudsters are clever,
but you are smarter

**December 2025**

Version Final

**© 2025 TransUnion International UK Limited**
**All Rights Reserved**

Registered in England & Wales with company number 3961870. Registered office: One Park Lane, Leeds, West Yorkshire LS3 1EP. Authorised and regulated by the Financial Conduct Authority.

This document is confidential. It is intended for the exclusive use of the individual or entity to which it was provided by TransUnion, and only for the purposes expressly permitted by TransUnion. It must not be disclosed, in whole or in part, to any third party without TransUnion's prior written consent.

The "tu" logo, "TransUnion", and other trademarks, service marks, and logos (the "Trademarks") used in this publication are registered or unregistered Trademarks of TransUnion LLC or their respective owners. Trademarks may not be used for any purpose whatsoever without the express written permission of the Trademark owner.

www.transunion.co.uk

# Table of contents

**Fraud Education for Students. Fraudsters are clever, but you're smarter ..... 4**

**Introduction to Fraud ..... 4**

Definition of fraud: ..... 4

Types of fraud young people are most vulnerable to: ..... 4

List of consequences and impact of committing fraud ..... 5

**Case Studies ..... 6**

Case study task sheet to complete. ..... 6

**Case 1: Meeting people online – Chloe's 'new friend' ..... 7**

Case study 1: Introducing Chloe ..... 8

Case study 1: Story | Chloe's "new friend" ..... 9

Case Study 1: Meet the Fraudster – The Friendly Faker ..... 10

**Case 2: Online Shopping and Scams – Olivia's 'bad purchase' ..... 11**

Case study 2: Introducing Olivia ..... 11

Case study 2: Story | Olivia's "bad purchase" ..... 12

Case study 2: Meet the fraudster – The strategist ..... 13

**Case study 3: Money Mules - Jack's #EasyMoney ..... 14**

Case study 3: Introducing Jack ..... 14

Case study 3: Story | #Easy Money ..... 15

Case Study 3: Meet the Fraudster – The Organised Crime Fraudster ..... 16

**List of organisations who help victims of fraud ..... 17**

**Action Plan for you to complete ..... 19**

**List of things you can do to protect your personal information online ..... 20**

**Organisations that help victims of fraud and what to expect them to do for you. ..... 23**

**Dictionary of terms associated with fraud ..... 27**

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Fraud Education for Students. Fraudsters are clever, but you're smarter

The resources in this handbook are designed to support the lesson you've had, about fraud, by providing the case studies, your action plan and checklists aims to protect your personal information. It also includes the organisations who can help and support you, should you become a victim of fraud. Remember you are not alone as there are lots of people and organisations who are there for you.

**TIPS FOR PROTECTION:**

Slow it down
Think it through
Overcheck
Pass it by someone

# Introduction to Fraud

## Definition of fraud:

- "Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person".
- This deception could have been through fake emails, a fake social media profile, a fake website, promise of goods that don't exist as advertised, or making bank payments.

Source: Report Fraud, Homepage https://www.actionfraud.police.uk/what-is-fraud

Words associated with fraud are:
Scams, scam alert, cheaters, impersonation fraud, hoax, stealing, ID theft, fake, scammed for someone else's benefit, forgery, money laundering, spoof, phishing, coercion, social engineering, cap rip-off, shady, grift, hustle, deception, , cooked

### Types of fraud young people are most vulnerable to:

1. Buying goods online and paying upfront known as Advance fee fraud
2. Banking and credit fraud including money mules
3. Scams, meeting people online, any online fraud is known as cyber fraud
4. Identity theft

**1. Buying online and paying upfront**
**Definition**: Advanced fee fraud is when fraudsters target victim to make advance or upfront payments for goods, services and/or financial gains that do not materialise

**Examples:**
Fake parcel delivery message,
Competition prizes/lottery e.g. you've won £1000, click this link to claim your prize
Ticket fraud e.g. you buy a ticket which is either fake or doesn't arrive
Online shopping and auction fraud e.g. you buy something online which doesn't exist or arrives but not as described

**2. Banking/credit fraud and money mules**

 © 2025 TransUnion International UK Limited. All Rights Reserved

**Definition**: Banking and credit card fraud happens when personal information is stolen from your debit, credit or store card, or the card itself is stolen, in order for money to be taken from your account or used to buy items in your name.

Links very closely to Identity theft and money mule fraud

Linked to banking fraud is money mule fraud. A money mule is somebody who receives illegitimate money into their bank account from someone they don't know, and then transfers that money to another unknown bank account on their behalf but keeps some of that money for themselves.

**Examples:**
Your bank card is cloned in the cash machine
You click on a link which asks for your bank details which you share
Fake investments into high interest accounts/stocks and shares/crypto currencies

**3. Scams, meeting people online, and any online fraud is known as cyber fraud**

**Definition**: Cyber fraud is any act of fraud that is committed through the use of computers and networks

**Examples**:

Phishing emails
Smishing text messages
Suspicious links which contain malware
Hacking into your account e.g. your social media accounts or bank account

**4. Identity theft**

**Definition**: Identity theft is when your personal details are stolen and identity fraud is when those details are used to commit fraud

**Examples**:

Hacking into your account e.g. your social media accounts or bank account

Stealing your identity from social media accounts

Sources: Crest, Understanding and addressing fraud against children and young people: An action plan, 2025.

And Report Fraud, identity theft definition, https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft

## List of consequences and impact of committing fraud

- Face a custodial sentence i.e. prison for up to 10 years
- Fined / forced to pay legal fees
- Thrown out of university or college
- Unable to get a job because you have a criminal record
- Unable to open a bank account
- Unable to get a student loan or loan to buy a car or things you want
- Emotional and psychological impact e.g. anxiety, depression, shame
- Lose friends, damage relationships

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Case Studies

## Case study task sheet to complete.

| | |
|---|---|
| Name of the case study | |

| Questions | Answers |
|---|---|
| What are the warning signs that something isn't right? | |
| What emotions did the victim feel? | |
| What things could the victim have done to help protect themselves? | |
| Who could have helped? | |
| Any other observations or comments? | |

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Case 1: Meeting people online – Chloe's 'new friend'

**The task:** Read Chloe's profile, the story and fraudster's profile to answer these questions.

Answer the questions at the end of the story:

- What are the warning signs that something isn't right?
- What emotions did Chloe feel?
- What things could Chloe have done to better protect herself?
- Who could have helped her?

## Case study 1: Introducing Chloe

Meet Chloe, a 17 year old college student who is eager to break into the fashion industry.



**Location**: Urban UK

**Education**: Sixth form A-levels

**Lifestyle**: Active on Instagram, TikTok, and Snapchat using iPhone or her Chromebook. She's trying to build her following and has her profiles set to public.

Her content is focused on TikTok dances to the latest music, fashion and selfies. Lately she's been posting about her new car and passing her driving test.

Chloe has a part-time job at a café to help pay for her online shopping (fast fashion, tech and accessories). She's got her own bank account and uses this to buy online items.

### Personality:

- Friendly and outgoing – loves making new friends online and wants to become a fashion influencer
- Trusting – tends to believe people who seem kind or share her interests
- Not very tech-savvy – doesn't fully understand privacy settings or data risks

### Online Behaviour

- Uses public Wi-Fi often and reuses passwords across sites
- Uses hashtags like #OOTD, #UKTeens, #FashionInspo #FashionTok
- Accepts friend requests from people with mutual interests and sometimes shares personal info in DMs (e.g., birthday, school name)
- Has Find My Phone which her dad setup but she's never logged into it herself

 © 2025 TransUnion International UK Limited. All Rights Reserved

### Why She's a Target

- Her public profile makes it easy to gather personal info
- She's flattered by attention from older teens or young adults
- She's unaware of synthetic ID fraud or how her data could be misused
- She's less likely to report suspicious behaviour out of embarrassment

## Case study 1: Story | Chloe's "new friend"

Chloe is contacted by Jay who seems charming and shares her interests in fashion and music on Snapchat. He's a little bit older, so it's really flattering, and he builds trust by taking an interest in her, asking questions about her school, subjects and her hometown. He lives not too far away but he can't meet her at the moment because he's busy with his new job. He regularly sends daily Snaps about his day, and she has shared her TikTok, insta and discord handles where he also likes her stories…but he never has time to go on video because of his new job.

Jay thinks Chloe is so beautiful and is always asking for selfies in her latest looks, though he prefers to just see her smiling face. He's just started working at a fashion brand PR company as an intern. He says his job is to find new talent to do collabs with two well known online fashion retailers , and he thinks she'd be perfect since her following is growing across TikTok and insta. He sends her a link to a fake brand collab opportunity form. She clicks the link and is taken to the fake website which looks professional and features lots of photos of people wearing the latest branded clothes. Chloe thinks Jay must be good at his job and is impressed. Jay says to get started she needs to pay a small fee and asks her to move money to his bank account. Eagerly, Chloe does that, it's not much money, only £50 and if this gives her the break, she needs to get into the fashion industry then what's the harm. Jay asks her for photos of herself, including some in her underwear, so that he can pass them onto the retailers. He the asks for more money as there are further fees to pay and said these needed to be paid immediately, as he was speaking with both companies later on that same day. He begins to manipulate Chloe, by making more promises that she's going to be a big hit with the online fashion retailers, Chloe is brimming with confidence and can't believe her luck! Unbeknown to Chloe, Jay is not the person she thought he was.

Jay has used Chloe's personal information taken from the form and her photos, to create a false identity which he's used to open bank accounts in her name. Jay had also used Chloe's personal information to gain access to her bank account and emptied her savings accounts. It's not until Chloe couldn't access her social media platforms that she realised something was very wrong.

It all happened so quick. Chloe couldn't believe she had been so silly to think this would give her the break she needed. Jay was so nice and helpful. Chloe felt violated. Confused. Embarrassed. Angry. She didn't know who to tell. Would they blame her? Would they understand?

### Why This Story Matters

Chloe's experience isn't rare. Young people are increasingly targeted by online fraudsters who want to steal your personal and banking information. It isn't personal. Fraudsters look for vulnerable people who they can befriend, manipulate and trick. The emotional toll can be devastating—shame, isolation, anxiety—and the financial impact can be life-altering where large sums of money have been stolen.

 © 2025 TransUnion International UK Limited. All Rights Reserved

## Case Study 1: Meet the Fraudster – The Friendly Faker

Fraudsters aren't always who we think they are, as in this example. Some fraudsters are opportunistic, while others operate within a crime gang, but all are perpetrators and committing a crime.



**Alias**: "Jay"

**Age: "**25"

**Location:** Unknown (possibly abroad or using VPNs) – frequently changing

**Platforms:** TikTok, Instagram, Snapchat, Discord, WhatsApp, Line

**Goal:**

- To collect personal information (like full name, date of birth, address, selfies, school name) to commit identity fraud or create synthetic identities.
- Poses as a peer or influencer
- Uses fake profiles with stolen photos
- Targets teens who are active online and appear independent

**Tactics Used**

- Pretends to be a teenager young adult
- Uses fake photos (stolen from influencers or AI-generated)
- Builds trust slowly: Compliments, shares fake personal stories, pretends to have mutual interests and seems to follow teens across multiple platforms like you would a friend
- Creates urgency or emotional pressure: "I need your help with something personal" or "Can you send me a pic for a photo shoot?"
- Offers fake opportunities: Modelling gigs, giveaways, or exclusive invites via phishing links or malware
- Exploits shame and fear to silence victims
- May impersonate brands or use deepfake tech

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Case 2: Online Shopping and Scams – Olivia's 'bad purchase'

**The task:** Read Olivia's profile, the story and fraudster's profile to answer these questions.

Answer the questions at the end of the story:

- What are the warning signs that something isn't right?
- What emotions did Olivia feel?
- What things could Olivia have done to better protect herself?
- Who could have helped her?

## Case study 2: Introducing Olivia

Meet Olivia a 16 year old student who loves online shopping.



**Name:** Olivia

**Age:** 16

Year 11 student at a mixed comprehensive school

Studying for GCSEs, including Business Studies and Computer Science

Wants to run her own business when he's older

### Lifestyle

- Lives with her mum and younger sister in a suburban area
- Has a part-time job at the local golf club working in the restaurant and uses her earnings to buy clothes, games, and tech online
- Enjoys music and gaming, and following influencers on TikTok and Instagram
- Often shops online for deals and limited-edition items, especially for albums by her favourite artists.

### Personality

- Friendly, curious, and independent. Has a small friendship group who she very much trusts
- Likes to stay on trend, especially with new music and values peer approval
- Tech-savvy – understands the importance of privacy settings
- Tends to act quickly when excited, especially when she thinks she's found a bargain

### Online Behaviour

- Active on social media platforms like Instagram, TikTok, and Snapchat
- Frequently clicks on ads and influencer links
- Uses public Wi-Fi often, uses a VPN and saves passwords on her mobile phone
- Often checks website URLs or privacy settings

 © 2025 TransUnion International UK Limited. All Rights Reserved

### Why Olivia Is a target of scams

- Trusts social media ads without verifying sources
- Eager to start saving for the future so that she can start her own business making him vulnerable to winning money in competitions
- Shares personal information (email, phone number, address) freely when entering competitions
- Limited awareness of how scammers use fake websites and phishing tactics

## Case study 2: Story | Olivia's "bad purchase"

Olivia was buzzing. She'd just finished her GCSE mocks and was pleased with her performance so wanted to buy a new pair of trainers. Scrolling through Instagram, she spotted an ad for a pair of limited-edition Air Jordan 4 Retro trainers – her dream trainers. The price? Just £75. Way below retail. She'd seen the same pair of trainers in the Nike store for £190.

The ad linked to a slick-looking website. It had glowing reviews, flashy photos, and even a countdown timer showing "only 3 pairs left." Olivia thought she best buy them quick before they sell out, but as Olivia browsed, a pop-up appeared:

> 🎉 Congratulations! You've been selected to enter our exclusive competition to WIN a £1000!! Just enter your name, email and phone number to claim your entry.

Olivia hesitated, but the site looked legit. She filled in the form and then entered her card details to buy the trainers.

A confirmation email popped up instantly. "Your order is being processed." But the tracking link didn't work. Days passed. No shoes. No updates.

Then things got weird.

Olivia noticed a £50 charge on her bank account for an online gaming site she'd never used. Then came the spam—texts, emails, even a call from someone claiming to be from her bank asking for more details.

Panicked, Olivia told her parents. They helped him contact the bank and report the fraud. Turns out, the website was a scam. Not only had Olivia lost her money, but the scammers had also stolen her personal information—her name, address, email, phone number, and card details—all from the fake competition and checkout form.

The bank cancelled her card and refunded the fraudulent charges, but the trainers? Gone. And Olivia spent weeks cleaning up the mess—changing passwords, blocking spam, and learning the hard way about online scams.

 © 2025 TransUnion International UK Limited. All Rights Reserved

## Case study 2: Meet the fraudster – The strategist

Fraudsters aren't always who we think they are. Some fraudsters are opportunistic, while others operate within a crime gang, but all are perpetrators and committing a crime.



**Name:** Linh

**Age:** 25

**Location:** Southeast Asia

**Education:** Has a degree in Art

**Platforms:** TikTok, Instagram, Snapchat, Discord, WhatsApp, Line

**Goal:** To collect personal information (like full name, date of birth, address, selfies, school name) to pass onto her manager, who commits identity fraud or creates synthetic identities.

**Lifestyle:**

- Live in a crowded apartment with other young workers in a city far from home
- Found it difficult to find a good job. Answered a job ad that promised a good career with a well-paid job, working for a digital design agency
- Works long hours  for an agency that is run by a criminal gang.
- Has no access to her personal documents such as her passport
- Receives minimal pay, most of which is sent back to family or used to 'cover living costs'

**Personality:**

- Quiet, intelligent and resilient
- Feels trapped and conflicted but remains hopeful.
- Fears the consequences of not doing a good job and feels conflicted with doing a good job and the fact  the ads and websites she designs are used for criminal activity
- Dreams of a better job and life

**Tactics used:**

- Works under supervision
- Creates and manages social media ad campaigns and websites used for phishing
- Translates campaigns and websites to target English speaking people
- Uses anonymized tools and VPNs to avoid detection
- Impersonating a brand or person

 © 2025 TransUnion International UK Limited.  All Rights Reserved

# Case study 3: Money Mules - Jack's #EasyMoney

**The task:** Read Jack's profile, the story and fraudster's profile to answer these questions.

Answer the questions at the end of the story:

- What are the warning signs that something isn't right?
- What emotions did Olivia feel?
- What things could Olivia have done to better protect herself?
- Who could have helped her?

## Case study 3: Introducing Jack

Meet Jack, the party animal whose just started university and realizing how expense things are.



**Name:** Jack
**Age:** 18
**Location:** Urban UK
**Education:** Sixth form A-Levels, now at university studying Business and Marketing
**Lifestyle:**

- Lives in student digs with his new flat mates
- Loves to party, go out and hit the nightlife
- Manages his own money and budget for the first time – rent, food, social life
- Getting to grips with independent living, away from his family
- Active on Instagram, TikTok, and Snapchat using his Samsung phone. Lately he's been posting about his university and life as a student. Lots of photos out drinking on fresher's week. His profile is set to public.
- Has recently got a part-time job in a local bar, has his own bank account and a student loan.

**Personality:**

- Friendly and outgoing – keen to make lots of new friends.
- Trusting of people quickly and open to new opportunities through his network
- Ambitious, loves the idea of a side hustle

**Online Behaviour**

- Uses public Wi-Fi often and reuses passwords across sites
- Uses hashtags like #UniLife, #FirstYearFeels, #CampusVibes, #FlatParty, #WinMoney, #CompetitionTime
- Accepts friend requests from people with mutual interests and sometimes shares personal info in DMs (e.g., birthday, school name)
- Has Find My Mobile activated but disabled it as soon as he got to university

**Why He's a Target**

 © 2025 TransUnion International UK Limited. All Rights Reserved

- His public profile makes it easy to gather personal info
- He is new to budgeting so may struggle financially so maybe tempted with money offers
- Trusting in nature so could be easily manipulated and coerced into doing something she doesn't really want to online
- Lack of experience, not understanding the consequences for moving money between unknown accounts
- Prone to fall for a scam, false job ad or false money making opportunity.

## Case study 3: Story | #Easy Money

Jack had just started university to study Business combined with Marketing. He was hoping to have a successful career in marketing, working with some of the world's biggest brands He was 18, excited, and adjusting to life away from home. He missed his family and pet dog Barnie. Between lectures, flat parties, and late-night study sessions, he was quickly learning that independence came with a price — literally. Rent, food, books, clothes and social life were draining his student loan faster than he expected. He'd even got a job working casually in a bar, but it didn't seem quite enough.

One afternoon, while scrolling through Instagram sat in the library, Jack saw a post that caught his eye:

"Want to earn £300 a week from home? No experience needed. Student welcome - flexible hours. DM us now!"

It looked like a student-run account. The comments were full of people saying how easy it was and that was all legit. Jack thought a job like that would fit perfectly around his studies, casual bar job and social life. Curious, Jack messaged them.

The reply came quickly:

"We're looking for payment processors. You'll receive money into your account and you'll forward it to our clients for us. It's totally legal and helps us manage international transactions. You'll get paid for each transfer."

Jack hesitated. It sounded strange, but he was desperate for cash. They asked for his bank details and said he'd get his first payment the next day.

Sure enough, £1,000 landed in his account. He was told to transfer £900 to another account and keep £100 as his cut. It felt easy. Too easy.

Over the next few weeks, Jack did more transfers. He started to feel uneasy—especially when the names on the accounts didn't match, and the people he was messaging became vague and pushy. There was such urgency to make the transfers straightway.

Then his bank froze his account. He couldn't buy anything, use his bank account or even his virtual card. That's when it hit home what he'd been involved.

Jack's bank fraud team had triggered an investigation and it transpired the money Jack had been moving was stolen—from phishing scams and fake online stores. Jack was now under suspicion of being a money mule.

Panicked, he contacted his university's student support team and his parents. With their help, he reported everything to Report Fraud and gave a full statement to the bank. He wasn't charged, but his account was closed, and he had to rebuild his financial reputation from scratch. Access to money became difficult and he was lucky not to have been given a criminal record which would have jeopardised his future.

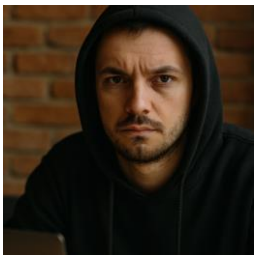
### Why this story matters

 © 2025 TransUnion International UK Limited. All Rights Reserved

Jack's story isn't rare. Young people are increasingly targeted by online fraudsters who want them to move money from an unknown account to another. It isn't personal and it's an easy trap to fall into. Fraudsters look for vulnerable people who they can manipulate and trick into helping them to 'launder money' across the banking systems. The emotional toll can be devastating—shame, anger, anxiety - but it's the damage it does to you generally, and possibly your family, if they are threatened. The consequences can be getting thrown out of univeristy, being unable to get a new bank account or student loan, or longer term, it affects your ability to rent a house or get a job. Money muling can result in a criminal record or jail, as you can be held legally responsible for moving stolen money.

## Case Study 3: Meet the Fraudster – The Organised Crime Fraudster

Fraudsters aren't always who we think they are. Some fraudsters are opportunistic, while others operate within a criminal gang to commit fraud at scale and often are funding weapons, human trafficking and drugs. All fraudsters are perpetrators and committing a crime.



**Name:** Alexei

**Age:** 32

**Location:** Easter Europe

**Education:** Studied computer studies at college

**Platforms:** TikTok, Instagram, Snapchat, Discord, WhatsApp, Line

**Goal:** To collect banking account information and make 'others' move money on their behalf. Wanting to move large sums of money across the banking system, without detection.

**Lifestyle:**

- Lives in a shared apartment with friends in a city with limited job opportunities
- Leads a mediocre lifestyle and isn't particular extravagant.
- Works irregular hours from home, uses multiple devices and VPNs
- Earns money through scams, cryptocurrency trading and selling stolen data. A career fraudster
- Motivated by financial gain and the challenge of scamming people

**Personality:**

- Intelligent, opportunistic and strategic
- Not physically threatening but thrives on emotional blackmail and manipulating others
- Sees fraud as a business, not a crime.
- Enjoys living on the fringes and staying ahead of the law

**Tactics used:**

- Prolific on social media to create profiles and target lists of people. Doesn't care about their age or where they live.
- Victims are recruited through online job ads, social media offering them 'easy money' or to work from home.

 © 2025 TransUnion International UK Limited. All Rights Reserved

- Builds relationships with people by manipulating them, lulling them into a false sense of security but then he asks for money because his mum is ill in hospital or he has an emergency.
- Purposefully shares suspicious links
- Messages people directly asking for personal information and their bank accounts
- Manipulates victims into opening new bank accounts in which to transfer money.
- Uses cryptocurrency to convert stolen money so it's harder to trace.
- Operates under different identities and has false documents such as driving licences

 © 2025 TransUnion International UK Limited. All Rights Reserved

# List of organisations who help victims of fraud

If you've been a victim of fraud, especially for the first time, it's completely normal to feel scared, confused, or even ashamed, but please know that you're not alone. Many people, including teenagers like yourselves, feel the same and remember it’s not your fault.

There are people and organisations out there who understand what you're going through and can help you. Whether it's reporting the fraud, getting emotional support, or learning how to protect yourself in the future, help is available. You’re not expected to handle this on your own— find somebody who can help, speak up, and let others help you through it.

**Definition:** A victim of fraud is somebody who has been intentionally deceived by another person, to gain something, usually money or personal information. This deception could have been through fake emails, a fake social media profile, a fake website, promise of goods that don't exist as advertised, or making bank payments.

**There are immediate measures you can take yourself to secure your personal information, your accounts or your device:**

- Change your password on the account that has been scammed and any other online account that uses the same password. Change those passwords every few weeks.
- Turn on two factor authentication on your accounts
- Turn on biometric authentication such as Face ID on your device and accounts
- Run anti-virus software to look for malicious code
- Freeze your SIM and mobile phone through your mobile phone provider
- Freeze or cancel bank cards in app or through your online account
- Set up privacy settings for your apps and online accounts, though your mobile phone. For example, Google provide lots of guidance on protecting your privacy.
- Constantly monitor your bank accounts, looking at larger and small payments. Report any transaction you don’t recognise
- Constantly monitor your social media accounts to check for things that are unusual or don’t seem right. Reject any friends requests from people you don’t know.
- When you are 18 years old, request a copy of your credit report from Transunion, Equifax and Experian. Check the information thoroughly including the ‘searches’ that have been conducted and report any that you don’t recognise.

**Tell someone**

- An adult
- A parent, guardian or another family member
- A friend
- A teacher
- A neighbour

 © 2025 TransUnion International UK Limited. All Rights Reserved

## Tell an organisation who can help

- Your bank, if you have lost money
- Your mobile phone company (VMO2, Vodafone, Three, EE, BT, Smarty, Tesco Mobile etc) if you have lost your phone, had your sim swapped or phone number transferred/blocked
- Your social media accounts by reporting using their in-site help
- Victim Support

## Report your fraud to an organisation who collects fraud information and can investigate – this is the right thing to do.

- Report Fraud
- The Police
- National helplines such as Childline, NCPCC, Victim Support or Citizens Advice
- Cifas – you can ask for a marker to be put against your name so that organisations such as your bank, know you have been a victim of fraud. The bank or other organisations might do extra security checks when you apply for credit. See the Cifas website for details of their Protective Registration service including charges.

## Share your story and experience to help and warn others. People such as

- Family
- Friends
- And post on social media (but not including your personal information!)

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Action Plan for you to complete

| **This is your personal action plan for what you would do if you were a victim of fraud** | |
|---|---|
| I would tell and speak to this person about what happened | Name of person or people you'd speak with. |
| Three things that I will do to stay safe online | 1.<br>2.<br>3. |
| Three things I will do immediately, after realising I am a victim of fraud? | 1.<br>2.<br>3. |
| My mobile phone details are:<br>IMEI number (type *#06# on your keypad)<br>Serial number<br>Make / Model | |
| **Keep this action plan safe** | |

 © 2025 TransUnion International UK Limited. All Rights Reserved

# List of things you can do to help protect your personal information online

### Protecting your personal information on your device

#### 1. Set Up Your Device for Security

Make sure your phone is prepared before you start using it. There are many things that you can do to help protect your personal information from being stolen from your device, or from someone else accessing your accounts.

- ✓ Enable **Find My iPhone / Find My Device.** Links here icloud.com/find, android.com/find and Samsung uses SmartThingsFind.
- ✓ **Back up your data** to the cloud or another secure location such as Microsoft OneDrive, Google Cloud, Apple iCloud or Dropbox.
- ✓ Use **anti-virus software** to scan and clean your device
- ✓ **Hide sensitive apps** (e.g. banking, email, social media)
- ✓ Use **strong, unique passwords** for each account. Strong passwords such as three random words or use a password generator. Avoid passwords such as QWERTY, 123456, the word password itself, names, dates or common phrases
- ✓ Use a **password manager** to store credentials securely. Popular password managers are 1Password, NordPass, LastPass. Obviously you need a really secure password to access the password manager.
- ✓ Set your device to **install updates automatically** to fix bugs and install patches
- ✓ Avoid storing personal info (like passwords) in **notes apps**
- ✓ Set up **Face or Fingerprint Unlock** through the Settings options.
- ✓ Set up **two factor authentication** for accounts that offer this extra security feature. It's easy to set up.
- ✓ Manage your **notifications** so that they don't appear on your locked screen to protect against shoulder surfers.
- ✓ Choose how long it takes for your **mobile phone or device to lock**. Under the settings menu your choose your preferred time.
- ✓ When downloading app, choose carefully which **features that app can access** on your device e.g. 'allow precise location', 'allow camera'.
- ✓ Tighten your **privacy settings** across all platforms by doing things like limiting who can see your social media posts.
- ✓ Write down you International Mobile Equipment Identity ( IMEI) , Make, Model and Serial Number. Type *#06# to find your IMEI number into your mobile phone keypad. The Make and Serial Number are printed on the back of your phone

 © 2025 TransUnion International UK Limited. All Rights Reserved

## 2. Stay Vigilant When Out and About

Follow these simple tips and you can protect your device and data in public spaces:

- 👀 Be aware of your surroundings—watch for **shoulder surfers** (people who get close and look over your shoulder to read your screen)
- 🧠 Stay alert and **trust your instincts**
- 🔒 Shield your **password, PIN, and FaceID** from view and set **pop up notification style** to **brief**
- 🌐 Use a **VPN** when connecting to public Wi-Fi
- 📱 Use a **privacy screen protector** or a **mobile phone lanyard** when walking in crowded places to reduce the likelihood of having your phone snatched

## 3. Signs your phone has been hacked

- 🔋 Battery drains quicker than normal
- 📱 Getting texts and One Time PIN codes you don't recognise
- 📱 Data usage is spiking
- 📱 Weird pop ups
- 📱 Apps disappeared or new ones appeared
- 📱 Locked out of your accounts
- £££ Money coming out of your bank account that you don't recognise

## 4. Spot and Avoid Potential Scams

Stay safe from fraud and phishing attempts when scanning social media, checking your emails or shopping online:

- 🚨 Treat unexpected messages or offers as **potential scams**
- 🛑 If something feels off, **STOP** — **S**low down, **T**hink it through, **O**vercheck and **P**ass it by someone such as a trusted adult or teacher
- 🚫 Be resilient—**don't give in to pressure** to make payments or buy something quickly
- ❌ You can **close a website or hang up** anytime
- 📵 Be wary of **unknown number calls** or text messages asking for money or personal information
- 🗣️ Make an excuse (such as "my dad is shouting me as my dinner is ready", "Nah I'm broke", "Sure - I'm just with my mum right now - she's in the police - will talk later" to **end suspicious conversations**
- 🔒 Look for HTTPS and the **two lines with a circle at the end** or padlock, in the browser URL to indicate the website is secure
- 💸 Don't fall for offers of **"easy" or "free" money**

 © 2025 TransUnion International UK Limited. All Rights Reserved

- Think long-term: is it worth risking your future for quick cash?
- Never share **PINs or bank access** with anybody
- Don't let others set up payments from your account
- Use **proxy or disposable emails** for sign-ups or one-time verifications. Popular providers are TempMail, 10 Minute Mail, Guerrilla Mail and Maildrop. Navigate to their website or download the App to create a time-bound email address
- Never share **PINs or codes**
- Avoid clicking on links in marketing emails— **go directly to the website** by doing a google search for that company or typing the web address directly into the browser
- Learn to spot phishing: look for **spelling errors, odd formatting, or incorrect logos**

## 5. Meeting People Online

Understand the risks and protect your future by being cautious as to who are friends with on social media and online.

- Keep your **social media private** and secure
- Don't accept **friend requests from strangers**
- Be careful who you **mutually follow or choose to follow**
- Check out the friends list when accepting a new friend request to see if you have common friends. Be wary if someone has only a few 'friends' or no photos and question if their profile picture looks real
- Notice if new friends messages escalate and come quickly, along with the subject of the messages, are they emotional stories or asking personal questions?
- ? Do friends and photos seem to check out? Check that their photos have other people in who are **tagged** and that they are tagged in other people's photos. **Can you find those** (often embarrassing) **photos that friends have been tagged in**?
- **Google image search.** Drag and drop the person's image into the image search box and it will show if that image has been used elsewhere
- Be careful when buying things from **Communities on What's app**
- Avoid sharing photos with **personal info** (e.g. school uniform, house number and address). Blur or crop out personal information.
- Don't share **intimate images** of yourself to people you've recently met online
- Be cautious about what you **post online.** Posting your photos whilst on holiday tells people you're away or photos from your birthday party can give away your date of birth
- Be wary of the **'Hi Mum or Dad' messages** from somebody claiming to be your child. Typically the person claims to have lost their phone or may ask for money. Examples: "Hi mum, I've lost my phone. This is my new number, can you What's App message me?" or "Hi dad, I'm in trouble and need money. Can you send me some money to help me out?"

 © 2025 TransUnion International UK Limited. All Rights Reserved

- **Meeting up?** If you decide to meet up, make sure it's in a public place and ideally take a friend along with you, just so you can double check that you're meeting the person you were expecting to meet!
- ❓ Ask questions—**be curious and sceptical**
- 🧠 If unsure, **stop and talk to someone you trust**

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Organisations that help victims of fraud and what to expect them to do for you.

| Who | How to report | What you can expect them to do |
|---|---|---|
| Your bank | Using a phone number found on the banks app, website or back of the bank card. | 1. They can freeze your accounts or bank cards.<br>2. They can monitor account more closely for suspicious activity<br>3. Help you get your money back. |
| Your mobile phone operator | Using a phone number found on the mobile phone operators website or app | 1. They can freeze your service and block the phone's IMEI to prevent further use. Ask for your mobile phone's IMEI number as this maybe asked for by the Police<br>2. Use Find My iPhone or Find My Device to locate it, remotely lock it and delete all data on it<br>3. Change all passwords used to access apps that you use on your phone including all social media, banking and email apps. |
| Report Fraud<br><br>UK's reporting centre for Fraud. Collate fraud intelligence on the National Fraud Intelligence Bureau (NFIB) database | Using their online tool reportfraud.police.uk) or call them on 0300 123 2040<br><br>Report Fraud http://www.reportfraud.police.uk | 1. They record your fraud loss and create a 'fraud case'. They will then give you a 'police crime reference number' which you can use to track your fraud case or provide to your bank.<br>2. They record your fraud loss on the NFIB database for recording and helping law enforcement agency investigations.<br>3. They assess your fraud case and possibly your local police force shall investigate, but they will keep you informed.<br>To report your fraud loss, you must create an online account. |
| Reporting fraud loss to an organisation who can investigate your scam, fraud loss, website or company that you used. | | |
| National Scam helpline.<br><br>Report a scam phone call from somebody claiming to be your bank. | Call 159<br><br>Charged at national call rate | 1. Calling this number will allow you to report the scam regardless of which bank you use.<br>2. They can work with other organisations to stop fraud as they can help shut down scam phone numbers, websites or accounts<br>3. Contact your bank if you received this type of call. |

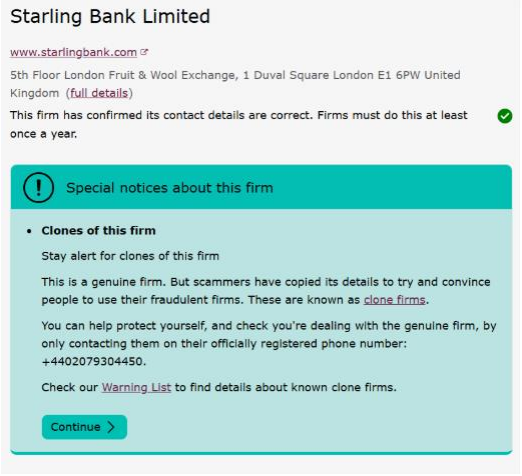
 © 2025 TransUnion International UK Limited. All Rights Reserved

| | | |
|---|---|---|
| Phishing emails<br><br>Emails that don't seem right or are suspicious can be shared for investigation | Email report@phising.gov.uk<br><br>No need to include a message, just forward the suspicious email | 1. The National Cyber Security Centre will record, investigate and scan the suspicious email automatically to check for malicious links, dangerous attachments, spoof sender address and phishing patterns<br>2. They may block the sender or take down any websites listed in the email to prevent others from receiving it.<br>3. If you clicked on any links in the email to log into a website, you should change your password that you used to access the website, run anti-virus scan on your device and report any financial loss to your bank. |
| Suspicious websites<br><br>Websites that don't look right or are suspicious can be reported for investigation | Fill in an online form: Report a suspicious website - NCSC.GOV.UK<br><br>https://www.ncsc.gov.uk/section/about-this-website/report-scam-website | 1. The National Cyber Security Centre will investigate the suspicious website and share with other organisations for possible further investigation<br>2. If the suspicious website is fraudulent then that website will be closed down<br>3. You should change any password you've used to access that website, run anti-virus scan on your device and report any financial loss to your bank. |
| Scam text messages<br><br>Text messages that don't look right or are suspicious can be reported for investigation | Send to phone number 7726<br><br>It's free from most UK mobile networks<br><br>No need to include a message, just forward the text message. | 1. The mobile phone network providers (e.g. VMO2, Vodafone, Three, EE, BT) will record and investigate the sender's phone number.<br>2. If the sender's mobile phone number is confirmed as fraud then that number will be blocked and shut down.<br>3. If you clicked on any link from within the text message you should change any passwords that you used to access the website, run anti-virus scan on your device and report any financial loss to your bank. |
| Scam phone call<br><br>An unexpected phone call from someone from your bank, asking you to move money or claiming to be from the fraud team | Contact your bank or Report Fraud by using an online tool (https://www.actionfraud.police.uk/reportscam) or call them on 0300 123 2040 | 1. Your bank will confirm if it was their fraud team which is unusual, who contacted you.<br>2. The bank will help you if you were tricked into sending money to somebody.<br>3. Report Fraud will investigate the details of the phone call and give you a 'police crime reference number' which you can use to track your fraud case or provide to your bank. |
| The police<br><br>To report any kind of fraud. | Calling the non-emergency number on 101 | 1. They record your fraud loss and give you a 'police crime reference number' which you can use to track your fraud case or provide to your bank.<br>2. Your fraud loss will be added to the National Fraud Intelligence Bureau database, where your fraud loss might be investigated. |

 © 2025 TransUnion International UK Limited. All Rights Reserved

| | | |
|---|---|---|
| | | 3. Your fraud loss might also be passed onto other organisations like Trading Standards to stop scammers or close websites down. |
| Trading Standards<br><br>If you bought something online which you didn't receive and couldn't contact the seller | To find a local office:<br>https://www.gov.uk/find-local-trading-standards-office | 1. They will investigate your complaint into the organisation<br>2. They won't be able to solve non receipt of your purchase, but they can close a business who is found to have scammed you<br>3. Contact Citizens Advice for advice. |
| Passport<br><br>If you have your passport stolen | Report online:<br>https://www.gov.uk/report-a-lost-or-stolen-passport | 1. The Passport Office will cancel your passport so that nobody can use it to travel<br>2. They will report it to the National Crime Agency who will report it to law enforcement agencies<br>3. You shall have to get a new passport and report your stolen passport to the Police. |
| Driving Licence<br><br>If you have your driving license stolen | Report online:<br>https://www.gov.uk/apply-online-to-replace-a-driving-licence | 1. The DVLA will cancel your driving license so that nobody else can use it<br>2. You shall have to get a new Driving License<br>3. You are required to report it to the Police. |
| **Registering your fraud** | | |
| Credit Reference Agencies | Contract all three of the UK's credit reference agencies (CRA's)<br><br>Transunion<br>Experian<br>Equifax<br><br>Only applies to those people 18+ | 1. Contact the customer helpline to tell them you have been a victim of fraud and to ask them to add a Notice of Correction (NOC) to your credit report<br>2. Ask each CRA for a copy of your credit report so that you can check the information held by them<br>3. If there is incorrect information on your credit report, then dispute the information with that CRA who will contact the company to whom the incorrect information belongs to and ask them to rectify it. |
| Cifas<br><br>To register yourself as a victim of fraud | Contact Cifas and ask for a marker to be put against your name to indicate you are a victim of fraud.<br><br>Using their online form:<br>https://www.cifas.org.uk/services/identity-protection/protective-registration/application-form | 1. Cifas record your details on their Protective Registration service using the details you provided. They add a marker or flag to your details to mark you as a 'victim of fraud'<br>2. They will keep this flag against your name for 2 years and there is a fee of £30.<br>3. Having a flag against your name may result in additional security checks being carried, should you apply for a bank account or other financial products during those 2 years. |
| **Checking a bank or company (such as a car insurance company) is genuine** | | |

 © 2025 TransUnion International UK Limited. All Rights Reserved

| | | |
|---|---|---|
| Companies House | Check to see if a UK company is real<br><br>https://find-and-update.company-information.service.gov.uk/ | 1. They keep a register of most l UK companies and check it is real, so that you can be confident that that company you are using is genuine.<br>2. They confirm the company you are looking for, has been confirmed as a real company<br>3. They provide address, company status, financial information and people details of each company who is registered. |
| Financial Conduct Authority<br><br>Check if a bank/building society or other financial services company is authorised . | Check a bank/building society or other financial services company<br><br>https://www.fca.org.uk/consumers/fca-firm-checker/search | 1. They keep a list of approved financial companies so you can check if they're real and trustworthy. This way, when you open a bank or savings account, you know the company isn't fakeThey warn you if that organisation (bank or building society) has been cloned.<br>2. It's free to use and anybody can check to confirm a bank, building society or other financial company is genuine.<br>3. This is an example from the register of a bank who has been cloned.<br><br> |
| Insurance Fraud Bureau<br><br>Report a false insurance company | Fill out their 'Cheatline' online form: https://www.insurancefraudbureau.org/insurance-fraud/fraud-types | 1. The Cheatline will investigate the suspicious website and share with other organisations for possible further investigation<br>2. If the suspicious website is fraudulent then that website will be closed down<br>3. Monitor your bank accounts to check no money has been stolen. |
| Motor Insurance Database | Check out their website: https://www.mib.org.uk/managing-insurance-data/what-we-do/ | 1. They will check the insurance policy you have been sold is genuine and not fake.<br>2. If it's fake then get yourself car insurance from a reputable organisation, if not you could have your car confiscated, you may be banned from driving or sent to court, fined and have points on your licence.<br>3. Tell your bank and monitor your account. |

 © 2025 TransUnion International UK Limited. All Rights Reserved

# Dictionary of terms associated with fraud

### Account takeover

- Is when someone accesses your bank, social media, email or mobile phone account without your permission. Once they have access to your account, they may change the details (such as password or mobile phone number), buy items that you didn't give permission for or use the information to pretend to be you to steal money from your friends, family or another company.

### Antivirus software

- A computer programme that helps protect your computer or device, from bad or malicious software that can mess things up or steal your personal information.
- Well-known companies who sell trusted antivirus software are: Bitdefender Total Security, Malwarebytes, McAfee, Norton Antivirus, AVG Antivirus for Android, Avast One, Microsoft Defender.

### Application fraud

- Is when someone lies or uses false or stolen information, to apply for something like a loan, credit card, or job to get money or benefits they shouldn’t have.
- Authorised Push Payment fraud (App fraud)
- This is when you are tricked into sending money to someone else who pretends to be your friend or the bank, but they are really a scammer or fraudster.

### Banking fraud

- Any scam that targets your bank account to gain access to your account without your permission or to pretend to be you and steal money from your account.

### Catfishing

- Is when somebody creates a false online account to try to be your friend, trick or scam you. It is often associated with romance fraud. (opp quiz)

### Clickbait

- Is prevalent on website or social media posts, where headlines are purposefully designed grab your attention, to urge you to click them, but the links can lead to scams or malicious websites.

### Crypto scam

- Is when fraudsters use cryptocurrencies (like Bitcoin) to promise big money or fake investments to steal your money.

### Cyber crime

- Any time of crime that happens online or using technology such as hacking, stealing information or spreading viruses/malicious computer packages.

### Cyber fraud

- Is when someone tricks or tries to steal your money or personal information online or using technology.

 © 2025 TransUnion International UK Limited. All Rights Reserved

### Deepfake

- Is a video that is created using AI, which looks real and sounds real.

### Delivery fraud

- Is when you receive a text message or email about a delivery or that asks you to pay for a postage fee that isn't real.

### eSim fraud

- Is when someone else without your permission, takes over your phone number digitally (i.e. without a physical SIM card) to access your account and steal your personal information.

### First party fraud

- Is when the personal themselves commits fraud i.e. it is you stealing the money or personal information or pretending to be someone else to commit fraud.

### Hacker

- Is when someone, without your permission, breaks into our mobile phone or computer to steal personal information, your money or to access your bank or social media accounts.

### Identity fraud / theft

- Is when somebody steals your personal information, like your name, address, date of birth, email or mobile phone number, with the intent to use these details to pretend to be you to open a bank account, get a bank loan or buy something online.

### Impersonation Fraud

- Is when someone else pretends to be you to open a bank account, get a bank loan, take out a mobile phone contract, buy concert tickets or buy something online.

### Investment fraud

- A scam where somebody promises to invest your money, to make you lots of money, but it is a fake investment. The fraudster steals your money, without investing it.

### Keystroke logger

- Is when a computer programme records everything you type – like passwords, messages or logging into your social media or bank account.

### Malware

- Bad computer programme that purposefully damages your device or steals your personal information.

### Money mules

- Is someone, who moves criminal money, on behalf of a fraudster or scammer, using your own bank account. As the owner of the bank account, you don't usually know where the money has come from, that you've been asked to move, or the person you are transferring the money to.

### Online fraud

- Is any scam that takes place online such as a fake website, a fake product that doesn't exist on a marketplace, a phishing emails, fake social media accounts.

 © 2025 TransUnion International UK Limited. All Rights Reserved

### Online marketplace fraud

- Is when fraudsters or scammers are using marketplaces such as Facebook Marketplace or TikTok Marketplace, to sell fake goods, or goods that don't exist or don't pay for goods.

### Pharming

- A scam that sends a link to a fake website, that looks real and so you enter your personal information and it's stolen by the fraudster.

### Phishing

- Is any email that tricks you to share your personal information or click a malicious link.

### Quishing

- Is a combination of a QR code and phishing. It's quick response code that you scan with your phone to instantly take a photo, which takes you to a website/app/form. That website/app/form is created by a fraudster to capture your personal information and you are tricked into thinking it's genuine.

### Ransomware

- Is a type of computer programme that is malicious and designed to block access to your computer or mobile phone. Typically the fraudster demands a ransom is paid to remove the ransomware and they are often spread through web links, phishing emails or devices without security updates.

### Romance Fraud

- When somebody pretends to be in a relationship with you, to gain your trust and steal your money. It's usually just online.
- Romance fraud is often linked to catfishing and sextortion.

### Scam

- Is when somebody tricks you to steal your personal information or money. Methods commonly used are phishing emails, fake websites, social engineering, malware, impersonation calls, phishing SMS messages, romance scams, false 'get rich' schemes or competitions, selling goods that don't exist etc.

### Sextortion (financial motivated)

- Is a scam, when somebody builds a relationship with you to gain your trust, and then they ask you to share intimate or embarrassing content (e.g. nude or sexual photos ) of yourself. The scammer demands money is paid to stop them from sharing the content you've shared.
- An example is when someone sends you a friends request on social media which you accept, and you build a relationship with that person who you come to trust. The 'new friend' then asks for intimate photos of yourself which you take and share with the 'new friend'. At which point they threaten to share the images with family and/or friends.

### Sim swap

- A scam where someone takes control of your mobile phone number, by tricking your mobile phone provider to give the scammer access to your phone. The scammer uses the personal information that has been stolen from you.

 © 2025 TransUnion International UK Limited. All Rights Reserved

### Smishing

- Is when fraudsters use text messages to trick you to share your personal information or share a malicious link.

### Social engineering

- When a fraudster manipulates and tricks you to share your personal information or financial information or do something that doesn't feel right. They may use emotional manipulation, pressurize you, be overly kind, make lots of promises they can't keep, bait you with opportunities and offers that are 'too good to be true', or offer you money to do something like share passwords, private information or do something risky.

### Spam

- Any unwanted message – usually annoying and can be used by fraudsters to share malicious links, links to fake websites or scams.

### Spoofing

- Is when a fraudster creates a replica website, email address or phone number, with the intent to trick you into trusting them.

### Synthetic Identity

- Is an identity that is made up of real and false information. Synthetic identities are often used by fraudsters to open a bank account, take out a mobile phone contract or commit any type of fraud (online or physically).

### Third Party Fraud

- Fraud committed when your identity is stolen by a fraudster and used to commit fraud such as buying a new mobile phone.

### Vishing

- Is when a fraudster calls you pretending to be from your bank or someone trustworthy, with the intend to deceit you to steal money or persuade you to share your personal information.

### Virus

- A type of malware that spreads across your computer or mobile phone that causes damage such as deleting files, stealing information,

### Voice cloning (AI)

- Is when a voice has been copied using AI, to sound like your family or friend with the intent of tricking you.

Source: of definitions: Based on a list produced by Crest, Understanding and Addressing fraud against children and young people: An Action Plan, pages 3-6 and Report Fraud website

 © 2025 TransUnion International UK Limited. All Rights Reserved