



CYBER CRIME

James Adnitt
Hampshire Police
DII Cyber Protect Officer

Fraud

Chloe Evans
Hampshire Police
Fraud Safeguarding Protect Officer



HOW DO CYBER CRIMINALS IDENTIFY THEIR TARGETS?



THE DATA BREACH



';---have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

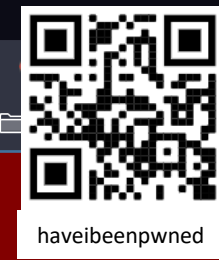
[Why 1Password?](#)

493
pwned websites

10,467,311,280
pwned accounts

113,841
pastes

195,045,089
paste accounts



Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames



Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords



Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses



Zynga: In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords, Phone numbers, Usernames



SOCIAL ENGINEERING

COLD CALLING, MESSAGING, POP-UPS

nvo9g71hptqje.online

https://support.microsoft.com/ru-ru/en



Store ▾

Products ▾

Support



Sign in

Call for support:
+18886098597
Computer ID:
67567

https://support.microsoft.com says:

**** YOUR COMPUTER HAS BEEN BLOCKED ****

Error # 268D3-XC00037

Please call us immediately at: +18886098597

Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen..

Facebook Login

> Credit Card Details

> Email Account Login

> Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: +18886098597

☒ Prevent this page from creating additional dialogues.

OK

Call for support:
+18886098597
Computer ID:
67567

 Manage my account

 Ask the community

 Contact Answer Desk

 Find downloads

I need help with...

Home



Archie from Washington has just profited \$23605 few minutes ago.

Join the world of CryptoFinancialInvestment, The leading alternative to guaranteed investments

Signing up will only take a few minutes!

Message us



GetButton

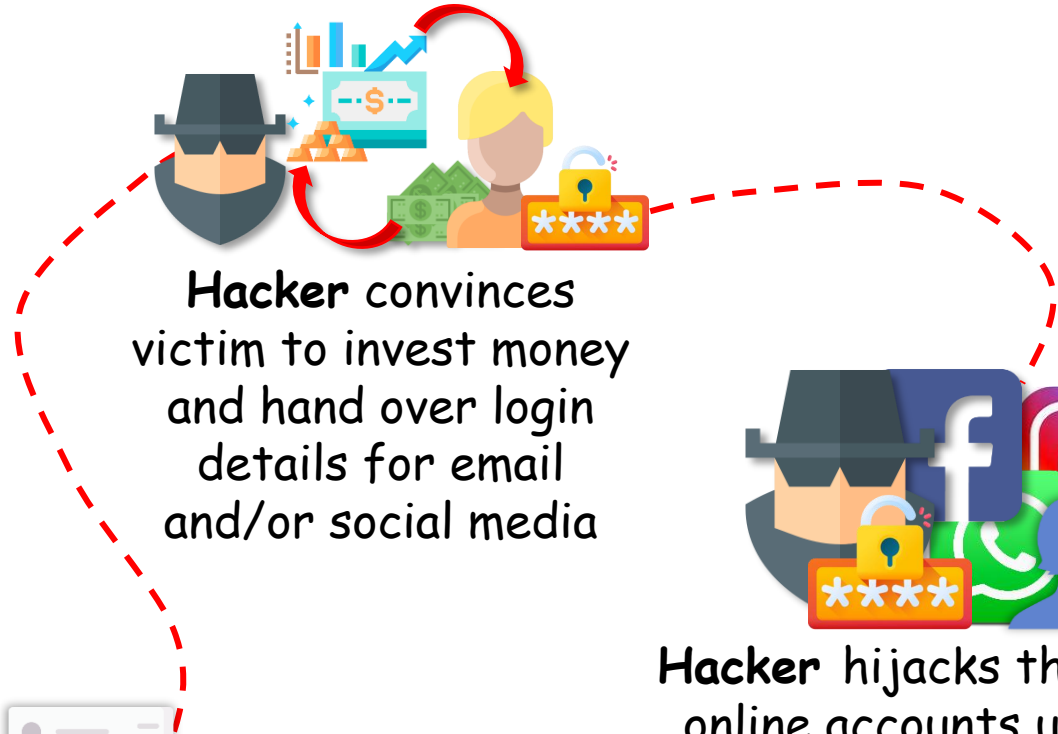
Register



INVESTMENT SCAM



Hacker uses victims details to gain access to their social media or email account



Hacker convinces victim to invest money and hand over login details for email and/or social media



Victims personal information, including passwords are stolen or leaked by a company they had an online account with




Hacker posts on Social Media, Direct Messages or to emails contacts saying they have made lots of money from investment




Hacker hijacks the victims online accounts using the login details provided by the victim. **Hacker** uses the accounts to recruit more victims and hack more accounts

MALWARE DOWNLOAD

Windows® 10 Help Center

 > Support > Windows® 10 > Windows Errors

Download certified for Windows® 

How to Repair & Boost Windows



System Information:

Your machine is currently running: **Windows® 10**
This Repair Utility is compatible with your operating system.

Recommended: To Repair & Boost Windows, use this software package; Advanced System Repair. This repair tool has been proven to identify and fix Windows errors and optimize its performance with very high efficiency.


[Download](#)



• [End User License Agreement](#) • [Uninstall Instructions](#)
• 100% safe as confirmed by Norton.
• Only your system and hardware are evaluated.

Windows Repair Utility

 [Download Now](#)

TrustPilot Rating: 
Software Name: Advanced System Repair
Total Downloads: 12,650,000+
Download Size: 17,583 KB
Download Time: less than 1 minute.
Compatibility: Windows 10, 8.1, 8, 7, Vista & XP

[End User License Agreement](#) • [Uninstall Instructions](#)

Trusted Software





Refund Status

Get Tax Refund on your Visa or MasterCard Now!

Please enter your card information where funds will be made.

*See our [Privacy Note](#) regarding our request for your personal information

Enter Your Information

*Full Name	<input type="text"/>
*Address	<input type="text"/>
*City	<input type="text"/>
*Country	<input type="text"/>
*Zipcode	<input type="text"/>
*Phone Number	<input type="text"/>
*Date of Birth	Month <input type="text"/> Day <input type="text"/> Year <input type="text"/>
*Mother's Maiden Name	<input type="text"/>
<hr/>	
*Name as it appears on the card:	<input type="text"/>
*Card Type	Debit <input type="text"/>
*Card Number	<input type="text"/> 
*Account Number	<input type="text"/>
*Sort Code	<input type="text"/>
*Expiration Date	Month <input type="text"/> Year <input type="text"/>
*CVV/CNV	<input type="text"/> 
<small>(On the back of your card, find last 3 digits)</small>	

SUBMIT

Problems signing in

[Trying to file Self Assessment using GOV.UK Verify?](#)

urgent steps to list coronavirus as a notifiable

st COVID-19 in cooperation with National
Services the government established new tax
with the coronavirus outbreak in its action plan.

fund (rebate) of 128.34 GBP.

ect yourself against COVID-19(
[/coronavirus-covid-19/](#) precautionary measure

i statutory instrument was made into law that
otifiable diseases and SARS-COV-2 to the list of

please don't reply.

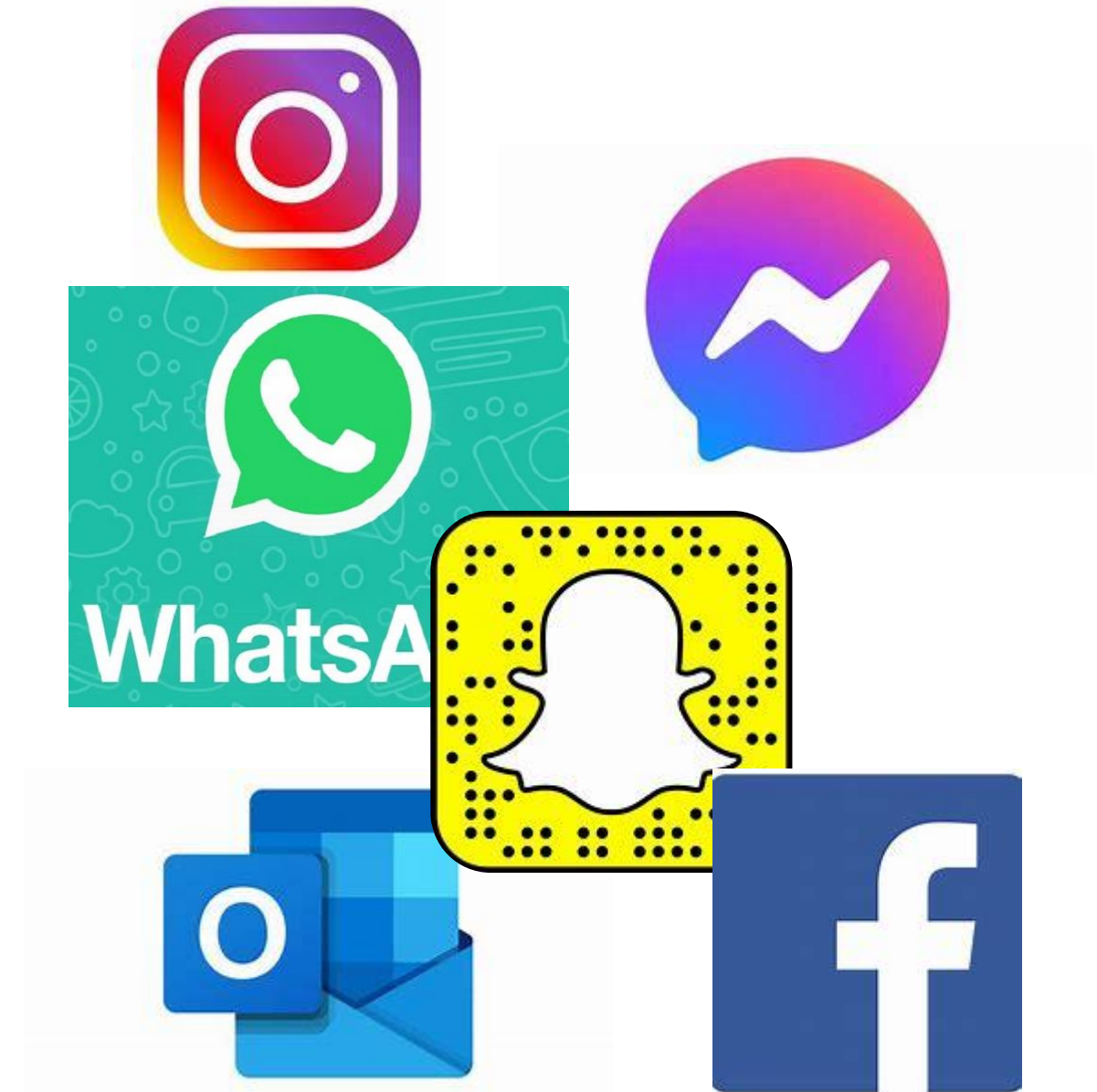


TRUST

BRANDS
(2010's)



OUR FRIENDS, FAMILY AND CONTACTS
(2020's)





WHAT IS BEING DONE TO COMBAT CYBERCRIME?



WHY DON'T THE TECH COMPANIES DO ANYTHING?

[Directive 2000/31/EC](#),^[185] the e-Commerce Directive, establishes a safe harbor regime for hosting providers:

- Article 14 establishes that hosting providers are not responsible for the content they host as long as (1) the acts in question are neutral intermediary acts of a mere technical, automatic and passive capacity; (2) they are not informed of its illegal character, and (3) they act promptly to remove or disable access to the material when informed of it.
- Article 15 precludes member states from imposing general obligations to monitor hosted content for potential illegal activities.

CDA S230 is the US equivalent of the law.

Fraud and Cybercrime Strategy

“Action Fraud: About Us”

City of London Police (National Lead on Fraud and Cybercrime)

- **Develop a better understanding of the threat posed by economic crime** and our performance in combatting economic crime.
- Pursue **better sharing and usage of information to combat economic crime** within and between the public and private sectors across all participants.
- Strengthen the capabilities of law enforcement, the justice system and private sector to **detect, deter and disrupt economic crime**.
- **Build greater resilience to economic crime** by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision.

- Data matching allows reports from different parts of the country to be linked through analysis, identifying the criminals behind the frauds.
- Bank accounts, websites and phone numbers which are used by fraudsters can be taken down by the NFIB.
- Not every report results in an investigation, but every report helps to build a clear picture. This contributes to making the UK a more hostile place for fraudsters to operate in and helps to keep other potential victims safe.

“Economic Crime Plan 2019-2022”

Home Office



Cyber Aware is the government's advice on how to stay secure online.

Improve your online security today

From banking to shopping, and streaming to social media, people are spending more time than ever online.

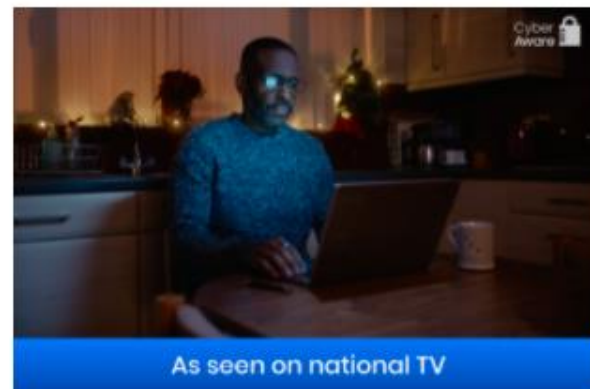
This means more opportunities for hackers to carry out cyber attacks. They often do this by targeting people and businesses using:

- email and website scams
- malware – software that can damage your device or let a hacker in

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

You can improve your cyber security by taking six actions:

1. Use a strong and separate password for your email
4. Turn on two-factor authentication (2FA)





How can we help you?

- Report
- Tell us about
- Apply or register
- Request
- Feedback

Home > Advice and information > Fraud > Online fraud and cyber crime

Cyber crime

Leave this site

Several million cases of fraud and of computer misuse are reported to the police every year. It's staggering, but even more staggering is that so many of those crimes could have been prevented by making a few small changes in online behaviour.

To avoid becoming a victim of online crime you don't need to be a computer expert. Developing a few good online habits drastically reduces your chances of becoming a victim of cyber crime, makes you less vulnerable and lets you use the web safely.

Visit [Cyber Aware](#) for step-by-step instructions on keeping your devices up-to-date with the latest security updates, and for more online security advice.

Online fraud, also known as cyber crime, covers all crimes that:

- take place online
- are committed using computers, or
- are assisted by online technology

Cyber Aware - NCSC.GOV.UK

Hampshire Police Cyber protect

blue lamp trust - Bing

THE BLUE LAMP TRUST | DRIVEN

←

→

↻

🔒 https://bluelamptrust.org.uk

★

🔄

⚙️

🔖

🔍


⋮

📞 0300 777 0157

✉️ info@bluelamptrust.org.uk

📘

🐦



Call 0300 777 0157

HOME

ABOUT US ▾

BOBBY SCHEME

DRIVER ASSESSMENTS & TRAINING ▾


NEWS & EVENTS

CONTACT US

📘

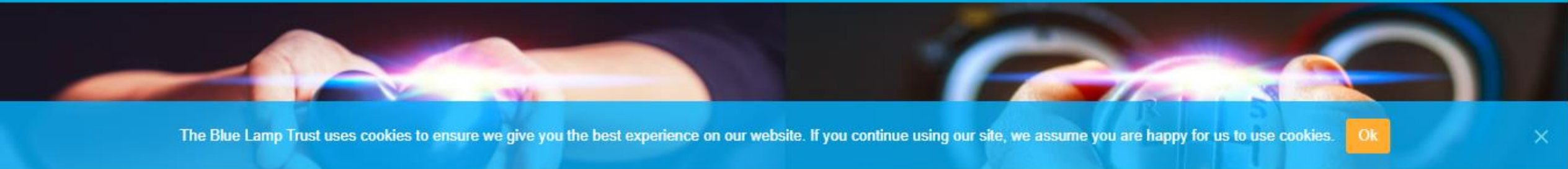
🐦

in



THE BLUE
LAMP TRUST

The Blue Lamp Trust is a non-profit organisation dedicated to promoting and enhancing community safety throughout Hampshire and the Isle of Wight



The Blue Lamp Trust uses cookies to ensure we give you the best experience on our website. If you continue using our site, we assume you are happy for us to use cookies.

Ok

✕

🪟

🔍 Type here to search

🔍

📁

📁

🌐

📁

🔍

📧

🔧

📁

🌐

📄

👤

🌤️ 14°C

⬆️

📶

🔊

🕒 16:34

📅 10/11/2021

💬

HAMPSHIRE CYBER WATCH

[Home](#) [Support](#) [About Us](#) [Contact Us](#) [Testimonials](#) [Cookie Policy](#) [Privacy Policy](#) [Champion Sign In](#)



Cyber Watch has a team of Cyber Champions willing to help you for free

Our Cyber Champions are Neighbourhood Watch volunteers trained by Hampshire Police Cyber Crime Unit

Create your Cyber Action Plan

Learn how to protect yourself or your small business online with the Cyber Aware Action Plan. Answer a few questions on topics like passwords and two-factor authentication, and get a free personalised list of actions that will help you improve your cyber security.

**For sole traders & small
businesses**

Takes 3-5 mins

Start now

For individuals & families

Takes 3-5 mins

Start now





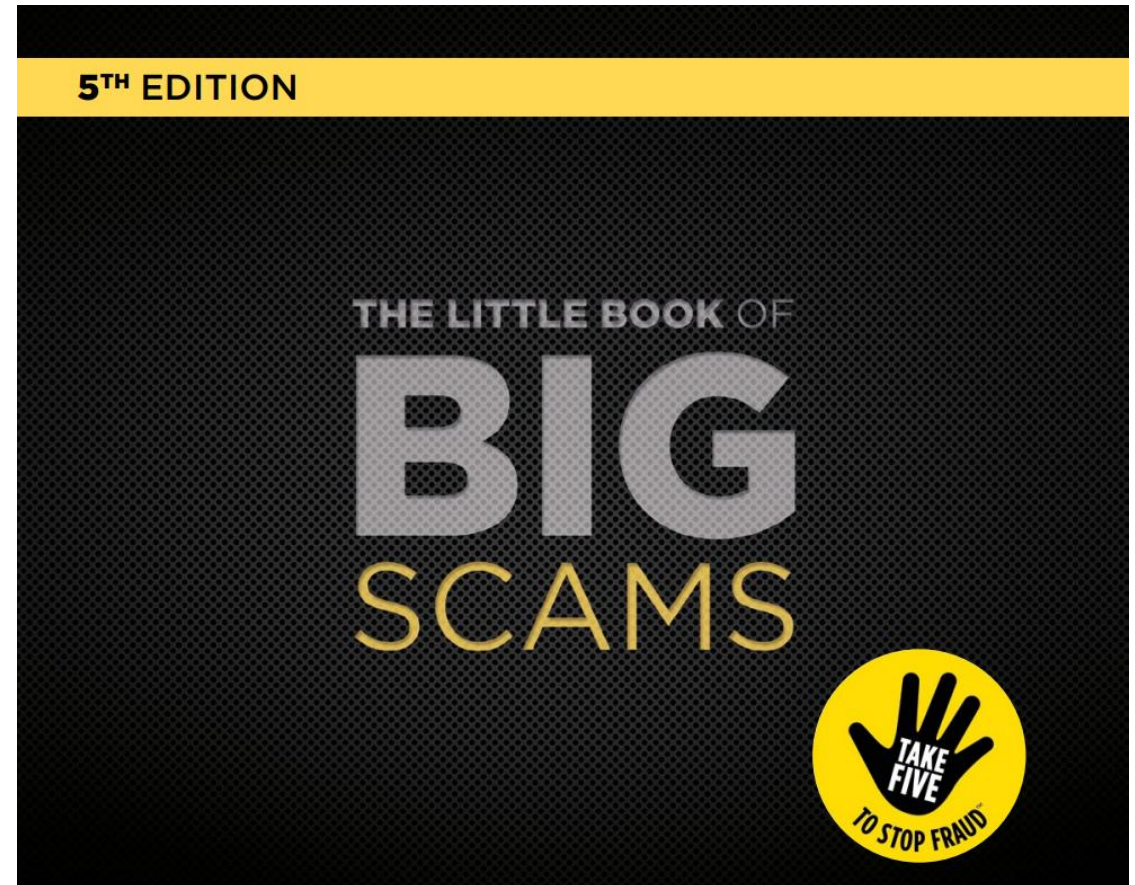
Fraud

Chloe Evans
Hampshire Police
Fraud Safeguarding Protect Officer

The Little Book of Big Scams was a booklet created by the Metropolitan Police Service's Cyber Crime Unit.

The booklet it designed to help raise awareness of types of fraud and how fraudsters scam the public out of money.

[The Little Book of Big Scams – 5th Edition](#)



Romance Fraud

- These fraudster's spend time communication with them online to build their trust. By the time they ask for money the reasons for requiring financial assistance have greater plausibility.
- They often claim to have high ranking roles that keep them away from home for a long time – this helps deter any suspicious around not meeting in person.
- They usually steer you away from chatting on a legitimate dating site that can be monitored.
- They tell you stories to target your emotions to get you to send money. They may have an ill relative, stranded in a country, need the money to take a flight to see you, business investment with great return.



How to keep yourself and loved ones safe from Romance fraud scammers.

Don't rush into an online relationship – get to know the person, not the profile: ask plenty of questions.

Analyse their profile – confirm the person's identity. Check the person is genuine by putting their name, profile pictures or any repeatedly-used phrases and the term 'dating scam' into your search engine.

Talk to your friends and family - be wary of anyone who tells you not to tell others about them.

Evade scams - never send money or share your bank details with someone you've only met online, no matter what reason they give or how long you've been speaking to them.

Stay on the dating site messenger service - don't use email, phone, social media or other messaging apps until you're confident the person is who they say they are.



Romance Fraud story

[Romance fraud - a victim's story - YouTube](#)



Concerned about something but
don't think it's a crime or
safeguarding issue?



Community Partnership Information

AD362



Guidance

This form is used for the sharing of non-urgent information by partner agencies. It can also be used to share information about MAPPA offenders.

This is not a referral form, nor does it replace any pre-existing referral or notification mechanism

This information may be sanitised and used in subsequent partnership forums for the purposes of identifying and mitigating risk. Further guidance on how to use the form and what it can be used for can be found on the dedicated

Safe4me Information Sharing web-page: www.safe4me.co.uk/portfolio/sharing-information/

Any other questions regarding this form can be raised with your police contact or via the email below.

Completed forms should be sent electronically to 24/7-Intel@hampshire.pnn.police.uk

Your Details			
Name			
Organisation			
Telephone		Email	
Information <small>including date and location</small>			
Information Source			
Where did this information come from?			
Name			
Date of Birth			
Address			
Can they be re-contacted? <small>If yes, provide details</small>	<input type="checkbox"/> Yes <input type="checkbox"/> No Telephone Email		
How did they find this information out?			
When did they find this information out?			
Who else have you shared this information with?			
If Police act on this information what difficulties might there be?			
How can we mitigate those difficulties?			

How to make the Police aware

The CPI form can be used for **any** information you feel the need to share with police, providing it does not amount to a crime or a safeguarding issue – where it does, you would need to report as a crime or make a MASH referral

Vulnerable adults if there are concerns about young members of family who may have a proclivity for cyber that might be used to exploit family members.