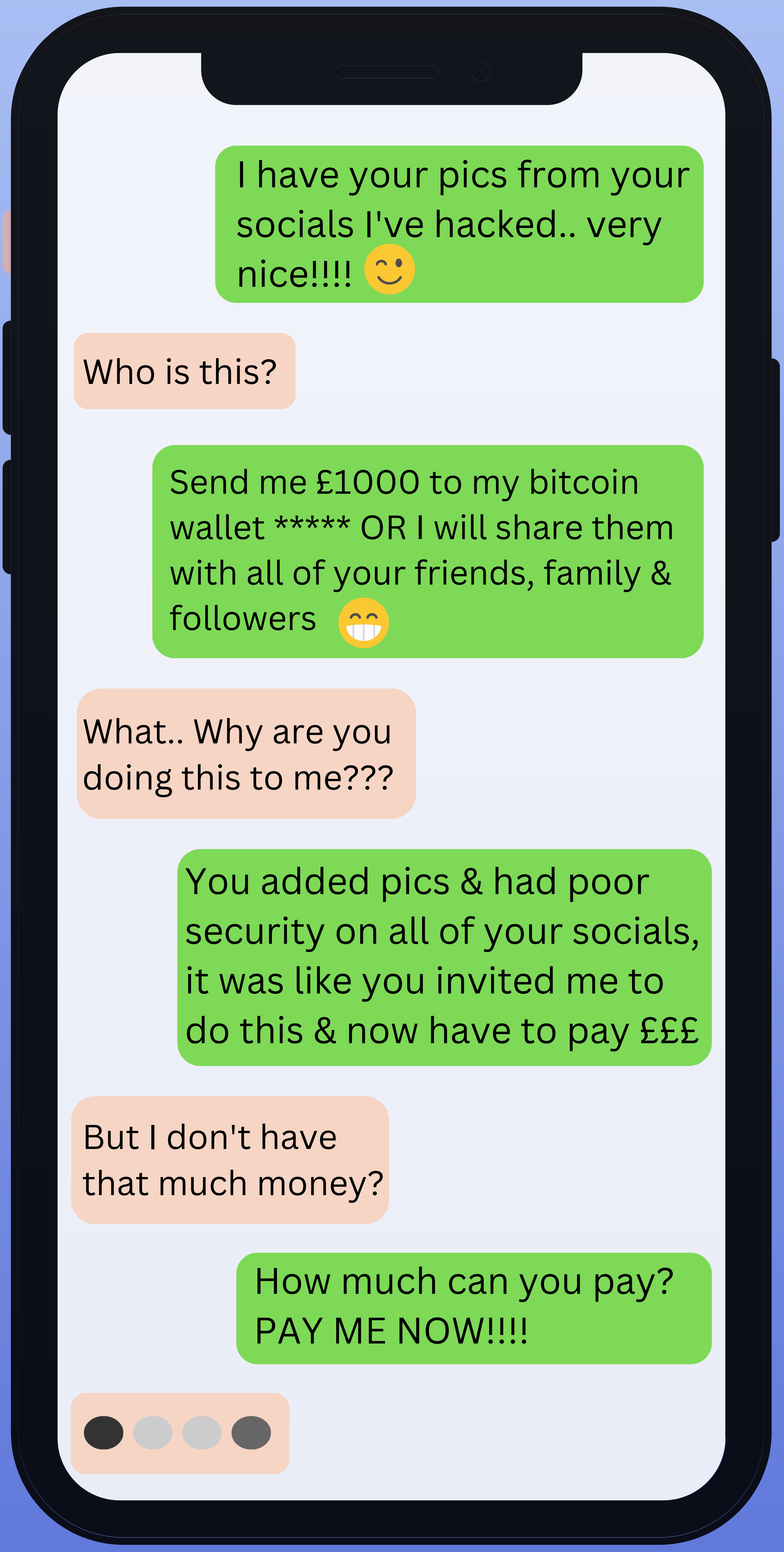
POLICE WARNING



I have your pics from your socials I've hacked.. very nice!!!! 🙂

Who is this?

Send me £1000 to my bitcoin wallet ***** OR I will share them with all of your friends, family & followers 😁

What.. Why are you doing this to me???

You added pics & had poor security on all of your socials, it was like you invited me to do this & now have to pay £££

But I don't have that much money?

How much can you pay? PAY ME NOW!!!!

This is sextortion.

Paying won't make it stop.

- ✓ Keep personal details & privacy settings updated
- ✓ Enable 2-step verification
- ✓ Keep passwords random using 3 random words
- ✓ Use different random passwords on each account
- ✓ For more information visit:

www.actionfraud.police.uk/sextortion

- ☒ **Don't** trust social media to save explicit images.
- ☒ **Don't** pay
- ☒ **Don't** respond to demands
- ☒ **Don't** think you're alone

A sextortion scam is when a criminal attempts to blackmail someone by an unsolicited message. The scammer will either claim they have login details, a video of the victim visiting an adult website or finding explicit images on the back of a hacking incident, and will then threaten to disclose these images unless the victim pays a ransom (usually in Bitcoin).

Sextortion incidents have included hacking of online accounts like social media and retrieving private images of their victim from the hacked account. It is important not to engage and do not do what they are asking. If an email has been received, the scammers behind these attacks do not know if you have a webcam or know if you've visited adult websites. Instead, they are attempting to scare their victims into paying a ransom and will send millions of emails in the hope that someone will pay. They'll often try to confuse victims by using technical details to make their email sound convincing. It may also include a password the victim has used.

Change any passwords that are mentioned or that have been compromised, do not engage, and report the incident through Action Fraud. If it’s an email, you can forward it to the NCSC's Suspicious Email Reporting Service (SERS): report@phishing.gov.uk, and then delete it.

Do not worry if your password is mentioned as it has likely been discovered from a previous data breach. You can check by visiting: https://haveibeenpwned.com/. This is why it is essential to use separate random passwords and not to repeat the same or similar password access multiple accounts.

Helping you stay protected online

EAST MIDLANDS
CYBER SECURE