This presentation was funded by the European Union’s Rights, Equality and Citizenship Programme (REC 2014-2020). The content of this presentation represents only the views of the Consent Ed Project and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Funded by
the European Union

Preventing online sexual harm

THE CONSENT ED. PROJECT

Who is an adult that you trust?

Think of an adult that you trust and could confide if you were to experience online harm.

Here are some examples:

- Parents or guardians
- Adult siblings or extended family member (aunt, uncle, cousin)
- Teacher, principal, SNA or school counsellor
- A friend’s parent that you have a good relationship with
- Sports coach or mentor
- Youth worker

How to tell an adult that you have been the victim of sexual harm online

Well done - you have taken a brave step!

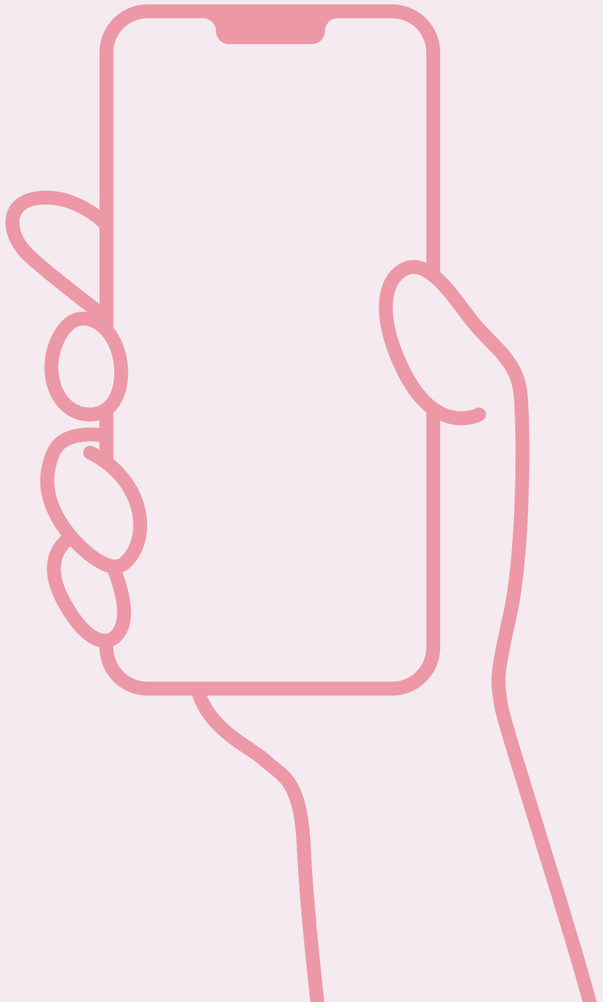
Telling someone what has happened can be really hard, but it's important that you seek out help from your trusted adult.

- Ask to speak with them in private. Explain that it is a sensitive topic you will be discussing.
- Sit with them and explain what has happened. Use examples and try your best to tell your story.
- Take your time
- Explain how it makes you feel
- If you have evidence (messages, screenshots, etc.) it might be a good idea to show them to the adult.

Screenshot the evidence

If you have been the victim of online sexual harm or harassment it is always a good idea to screenshot the nasty comments or exposure because sometimes the person behind them might delete them.

Save screenshots in a safe place and share them with an adult that you trust.



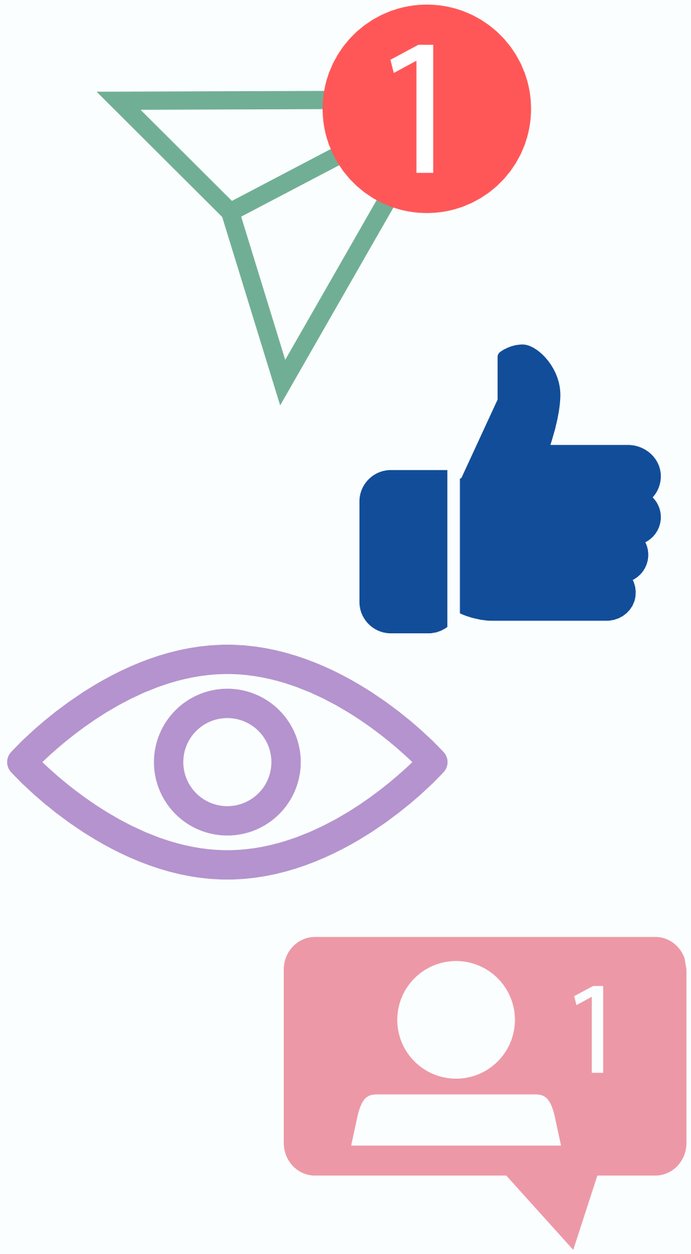
Followers and friends

It is important that you know each person that follows you in real life.

Sometimes a business, meme or ad account may follow many personal accounts, but we don’t know who is *actually* running the account - yet they can see all information that we share online.

Use story settings to hide your story from people you don’t know or trust, so that only people you know well can your private life.

If someone makes you feel uneasy or unsafe online, restrict them or block them.



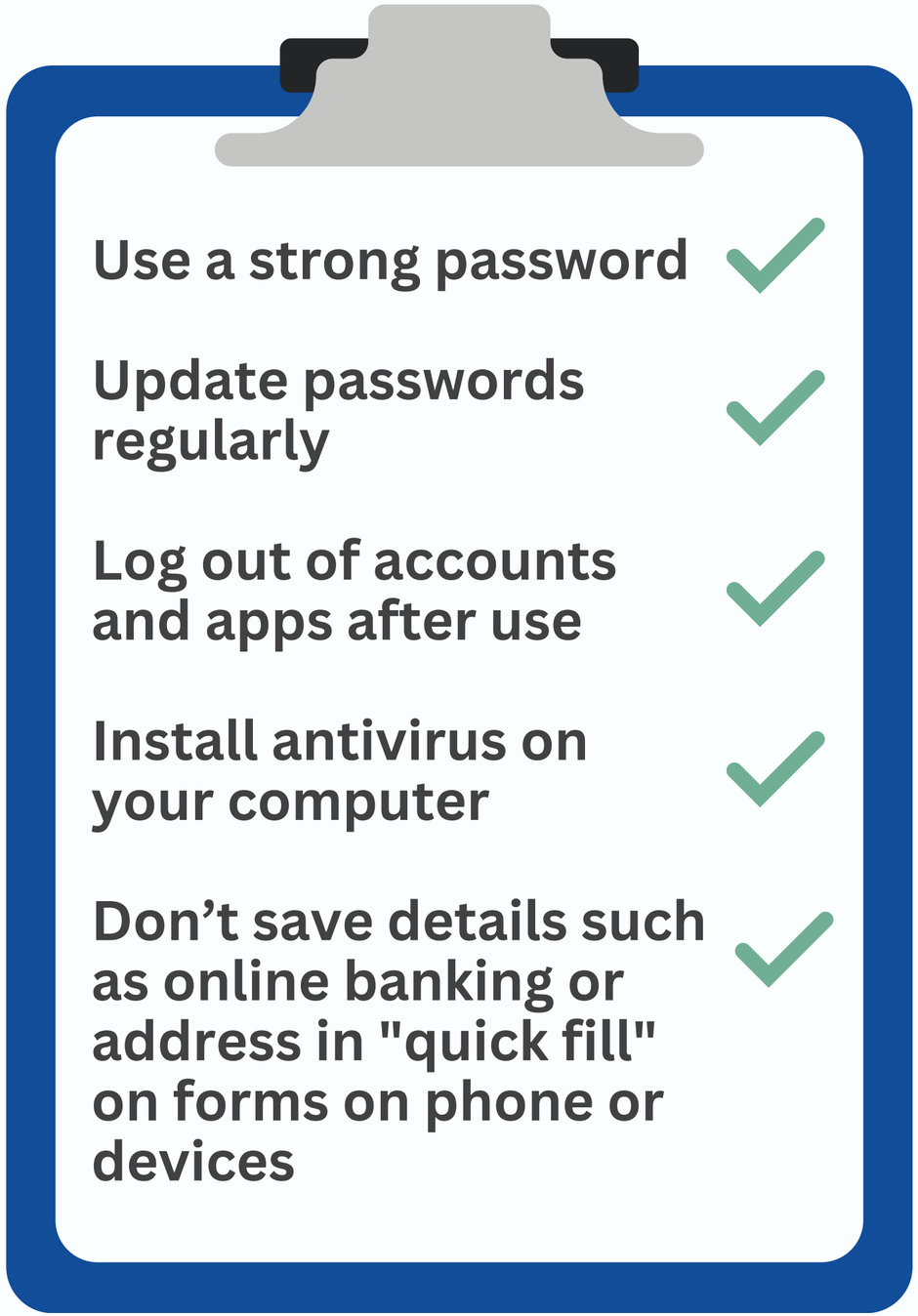
Doxxing - how to avoid it

- **Use a VPN -** A virtual private network can help you shield your personal information from doxxers. A VPN will hide your IP address, and hackers won't be able to get this address for your location or other personally-identifying information.
- **Use strong passwords -** Avoid using the same password for multiple accounts, especially ones that may have financial information or your address.
- **Protect your devices and accounts** using multi-factor authentication whenever possible.
- **Beware of phishing emails -** Be wary of emails that supposedly come from your bank or social media accounts. If you're ever unsure about an email, look up the sender they claim to be, or don't answer it (if it's legitimate, they'll contact you again!
- **Avoid oversharing -** Don't overshare on social media, online forums, or message boards.
- **Avoid third-party login options.**

Know the signs - hacking

- Strange or inappropriate pop ups
- Messages opened that you didn’t open
- Apps used that you wouldn’t usually use
- New apps installed
- Texts and calls not made by you
- Phone performing slowly
- Password change prompts

How to protect yourself from hacking



Location settings

- Turn off location settings apps you may share private information on, that may lead you to be in a dangerous situation. If you need your location settings on, set them to only be turned on while using the app.
- Only have your location turned on for friends and family.
- Be aware that using geotags on social media or "checking in" at a location may let someone know where you are or where you live.
- Never share your home address online.

Catfishing: what to look out for

Vague information: a catfish will be very vague or inconsistent about details in their life, so as to not catch themselves in a lie.

Photos: few candid photos, overly photo-shopped or retouched images, or only having one profile photo can be a sign of a catfish.

Only communicates via texts or DMs: a catfish will make excuses to get out of sending selfies, videochatting, or speaking on the phone.

Asking for or giving you things: either asking you to send them money or by sending you money a catfish may shower a victim with presents to win them over

A sparse social media account: having minimal posts or likes on their account or having few friends or interactions with their account

Use a common sense approach: if it seems to good to be true, it probably is.

Online Safety - summary of top tips

- **Create strong passwords –** Do not share passwords even with people you trust. Do not use same password for all apps.
- **Use multi factor authorization settings for all apps.** Log out of apps if not in use for long period of time.
- **Limit the amount of personal information you share.**
- **Make sure that you know all your friends and followers in real life,** do not accept someone you do not know.
- **Do not share any details that identify where you live or where you attend school** (be careful not to share snaps/photos in school uniforms).
- **Report any incidents that may occur.**

This presentation was funded by the European Union's *Rights, Equality and Citizenship Programme* (REC 2014-2020).