

Online crime is always personal

Don't be a target.



IT'S ALWAYS
PERSONAL
DON'T BE A TARGET FOR AN ONLINE CRIMINAL

www.getsafeonline.org

Has anybody ever tried to tell you that online crime isn't personal, because the internet is so vast and criminals don't care who they target?

Don't believe it!



Online crime: it's always personal



Here's why:

- Criminals personally target individuals like you, your family or your business via data they have such as your email address, phone number or social network page.
- They also gather together all the snippets of personal information you innocently put online, like your birthday, your kids' names, your national insurance number and your login details. That could all be all they need to defraud you or steal your identity... with disastrous results.

Today's cyber criminal has the technology and ingenuity to watch and wait for you to reveal too much information. You could be targeted, however careful you think you've been on the internet, or on the phone.



Don't give online criminals the ammunition to target you online.



With some simple precautions and common sense, you can keep yourself, your family, your finances and your workplace safe.



Try these tips for starters:

Six top tips to keep it personal

1. Don't publish your date of birth in your profile or highlight your birthday in posts or tweets. Why not? **Your date of birth is very useful information for a fraudster, hacker or identity thief.**
2. Remember that if you use the names of pets, family members, a sports team or other 'favourite' things in your passwords or memorable words, and reveal your likes and dislikes online, **you may be handing a criminal clues to your login details.**
3. **Don't reveal your passport number, driving licence number or any other official details** to anyone unless you're absolutely sure that they are authentic, and that providing these details is necessary. For example, if a prospective employer or agency asks you for a passport scan as proof of ability to work in the UK, check their authenticity.
4. Don't get fooled into revealing your **PINs or passwords** in response to an email, social networking post, text or phone call, however convincing it seems that the request is from your bank, the police or another real organisation.
5. Don't write down or store **login details** electronically or on paper, where there's a chance they could be found.
6. Never open an **email attachment** unless you're 100% certain of who sent it, or what it is. This is because it could contain a virus that steals your personal information. Even an email that seems to come from a friend or colleague could have been sent by a virus on their device. If in doubt, ask the person you believe sent it before opening anything.



IT'S ALWAYS
PERSONAL
DON'T BE A TARGET FOR AN ONLINE CRIMINAL

To get the full story on how to protect yourself against becoming a target for an online criminal, visit www.getsafeonline.org



About Get Safe Online

Get Safe Online is a joint initiative between the Government, the National Crime Agency, and public and private sector supporters from the world of technology, communication, retail and finance to raise awareness of internet security, and help individuals and smaller businesses in the UK to use the internet confidently and safely.



www.getsafeonline.org

OFFICIAL PARTNERS

