

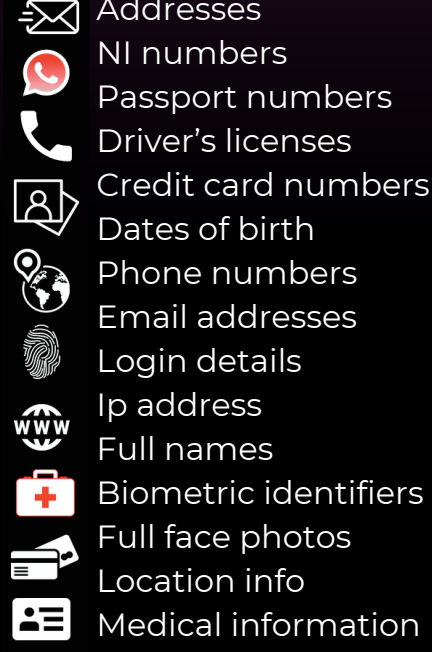
GDPR and Mobile Devices

Think about GDPR every time you use your mobile phone for work

GDPR's 'Security Principle' requires data to be...

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss..."

What **Personal Data** can you access on your phone right now?



- Addresses
- NI numbers
- Passport numbers
- Driver's licenses
- Credit card numbers
- Dates of birth
- Phone numbers
- Email addresses
- Login details
- Ip address
- Full names
- Biometric identifiers
- Full face photos
- Location info
- Medical information

Consumers value privacy and data protection



When a business has had a breach in the past, 70% said this would be a concern and affect their trust levels.



61% of companies don't protect data on employee mobile phones

Data from: Deloitte, 'A New Era For Privacy GDPR six Months on' and The Economic Value of Prevention in the Cybersecurity Lifecycle, Ponemon Institute LLC

GDPR breaches happen to all types of business

Businesses can be fined the higher of

€20M
or **4%** of
ANNUAL TURNOVER

for a GDPR breach

PHISHING

(3,091)

was the biggest cause of all the cyber-related data breaches reported to the ICO in Q4 2021-22

Followed by

UNAUTHORISED ACCESS

(1,449)

and

RANSOMWARE

(1,373)

Phishing incidents mostly affected these sectors:

Health (5,632)

Education & Childcare (4,172)

Finance & Insurance (2,874)

Local Government (2,750)

Retail & Manufacture (2,519)

General Business (2,513)

Legal (2,332)

Every year cyber security attacks lead to breaches of GDPR. These reported attacks happen in all industries. You need to protect every device, including phones and tablets.



Employees increasingly use mobile devices for work. If mobile devices can access company data from the cloud, company servers or locally, those devices then become a potential cause for a data breach... and if your mobiles are unsecured, they're an easy target for a cyber attack.

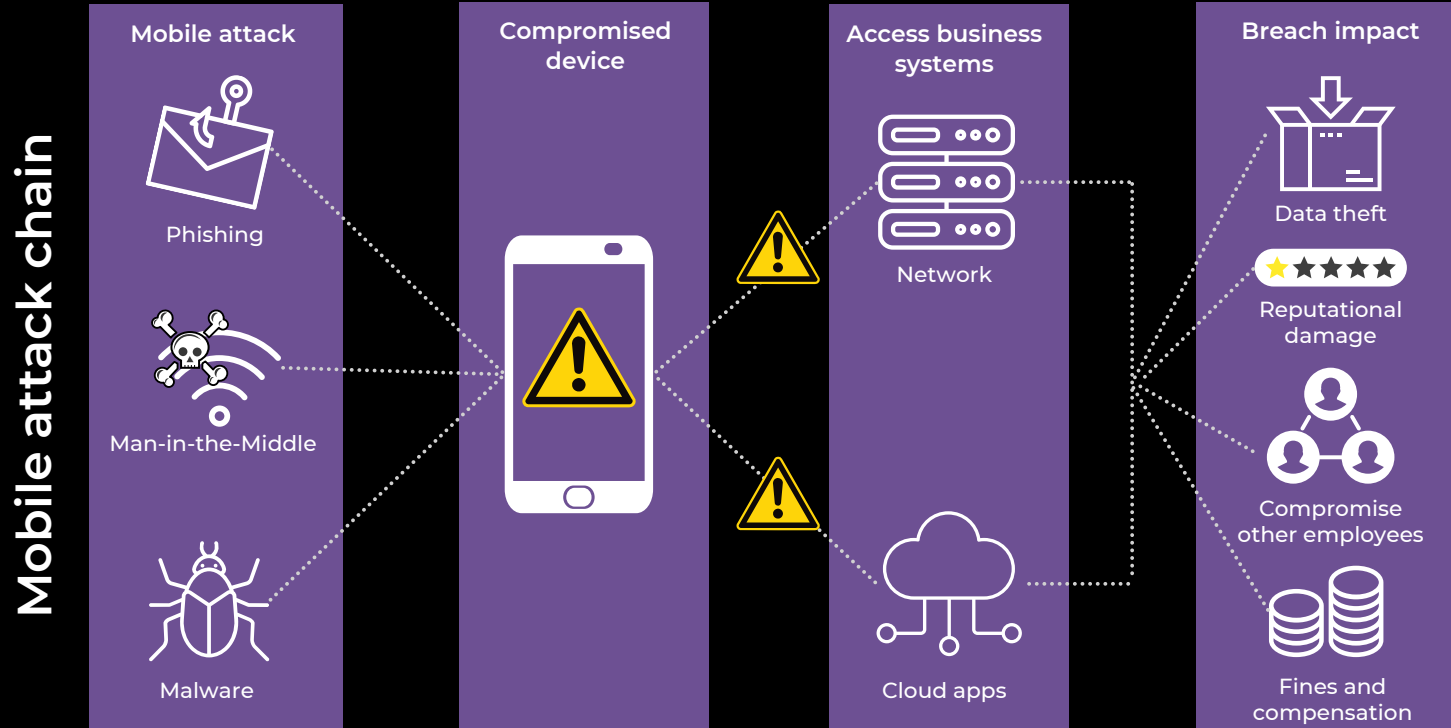
Ben Jones, Co-founder and CEO of Traced

Data threats on mobile devices

Phishing attacks and unauthorised access (such as by hacking or leaked passwords) are some of the biggest causes of data loss.

Mobile phones and tablets are particularly susceptible to these kinds of threats:

- apps may carry viruses or malware
- it's easy to fall for a phishing attack on a small screen with less contextual information
- patches for operating systems aren't rolled out to all devices at the same time
- devices connect to lots of WiFi networks, some of which may be compromised.



How does Trustd MTD keep your data safe?

Trustd Mobile Threat Defense (MTD) ensures appropriate security over the personal data that your mobiles can access.

Blocks phishing and malicious websites

Detects Malware & Spyware apps

Supports Zero-Trust access to data

Reveals device vulnerabilities and outdated OS

Identifies compromised WiFi networks

trustd

Privacy-first Mobile Threat Defence from Traced

