WHITE PAPER

IT STARTED WITH A PHISH...

Busting common myths around mobile phishing

trustd MOBILE

Why mobile is the best place to go phishing



__73%__ of organisations __suffered a breach__ from their mobiles over the past year in 2026 and __42% of them were from phishing__.

Trustd Mobile Threat Crisis Survey - 150 Cybersecurity Leaders in 100-10k employee orgs 2026.

With employees increasingly relying on personal devices for work, mobile threats are no longer a danger to an individual device, but a danger to your business.

Mobile phones are often a gateway to multiple business systems including email, and numerous Cloud-based apps and services — as well as multiple personal messaging apps.

Those messaging apps make smartphones a prime target for phishing. And most mobile phishing attacks avoid email, so traditional email-based filtering can't stop them.

Mobile phishing is escalating: 85% of organisations say mobile attacks are increasing and 80% have experienced mobile-phishing attempts against employees. When organisations tested their staff with simulated smishing, almost half found that more than one in four employees clicked.[1]

Whatever your mobility strategy, or your split between Apple and Android, phishing is one of the biggest mobile-borne threat to your data.

1 Verizon 2025 Mobile Security Index, pp. 6 and 9

Mayhem and malware

The first link in the chain of attack

Phishing has persisted because it is cheap, effective, and versatile: It can be used at scale, in massive email or SMS campaigns, or in targeted attacks against specific individuals.

Phishing is often the first step in an attack against an organisation. Criminals use it to steal passwords they can use to access internal business systems, or to gain personal information that can later facilitate a successful spear-phishing attack.

82% of phishing attacks targeting mobile in 2024

Zimperium

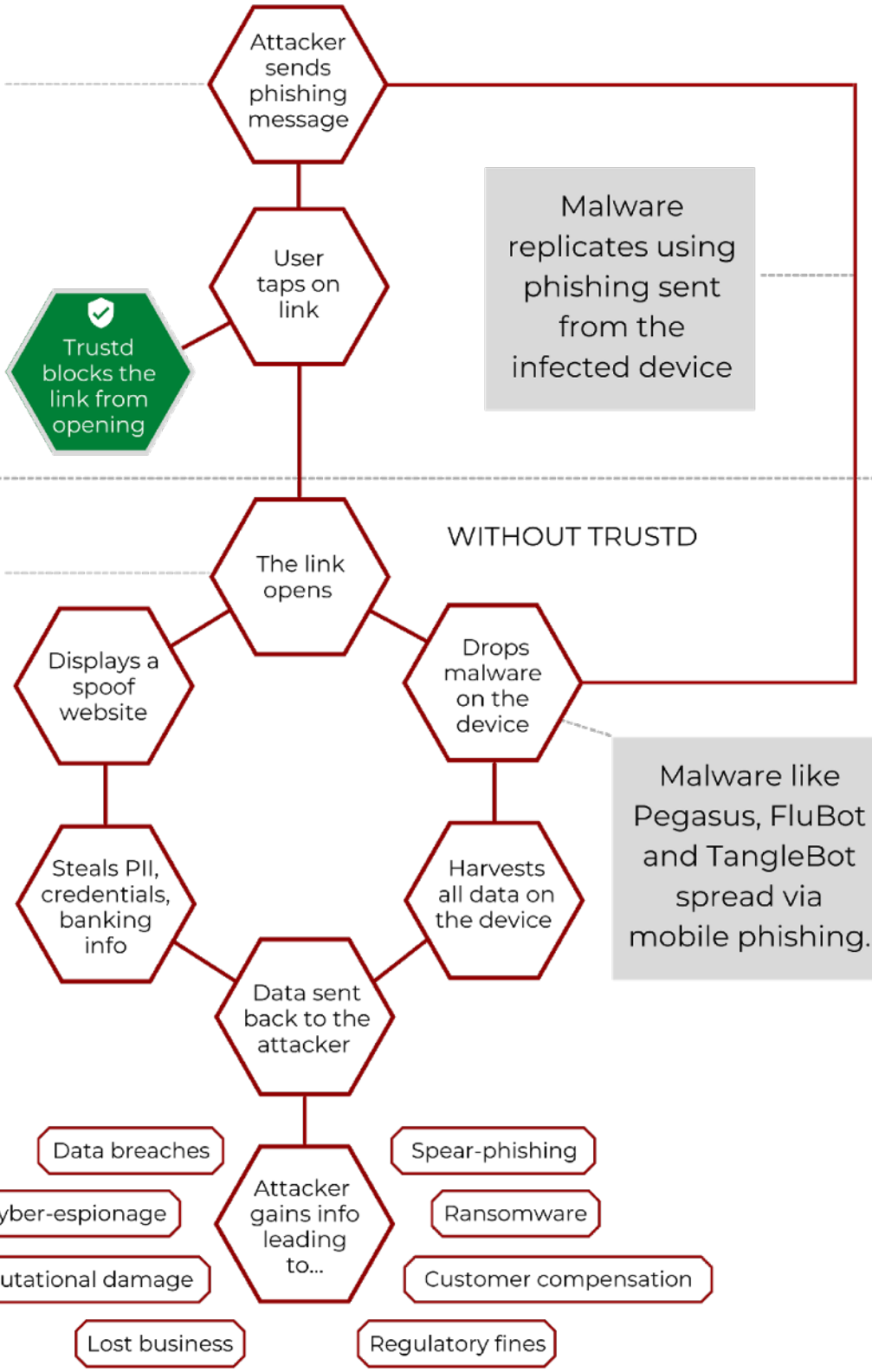
A successful phishing attack can lead to:

- **Unathorised access** to data and critical business systems,
- **Malware** such as spyware, keyloggers or banking trojans,
- **Ransomware** that encrypts files and demands payment to decrypt them,
- **Social engineering** that can result in huge financial transfers, and ultimately, to
- **data loss, fines and loss of reputation**.

The Mobile Phishing Killchain

It starts with a phish

Phishing can be sent via links in email, SMS, messaging apps, social media, websites, etc



Malware replicates using phishing sent from the infected device

Mobile phishing links lead to one of two types of threat. Both are designed to ultimately steal personal information.

Malware like Pegasus, FluBot and TangleBot spread via mobile phishing.

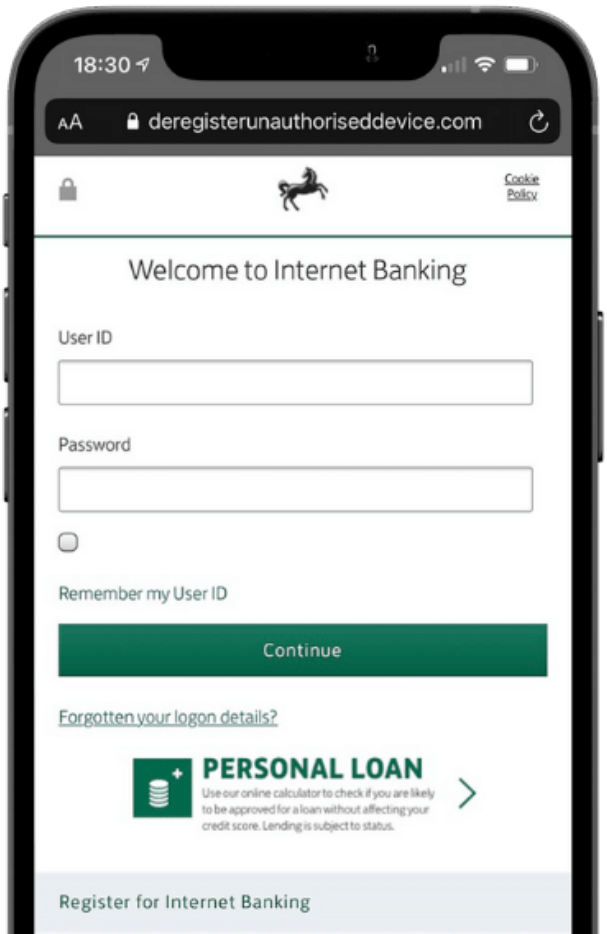
© 2026 Traced Ltd. All rights reserved.

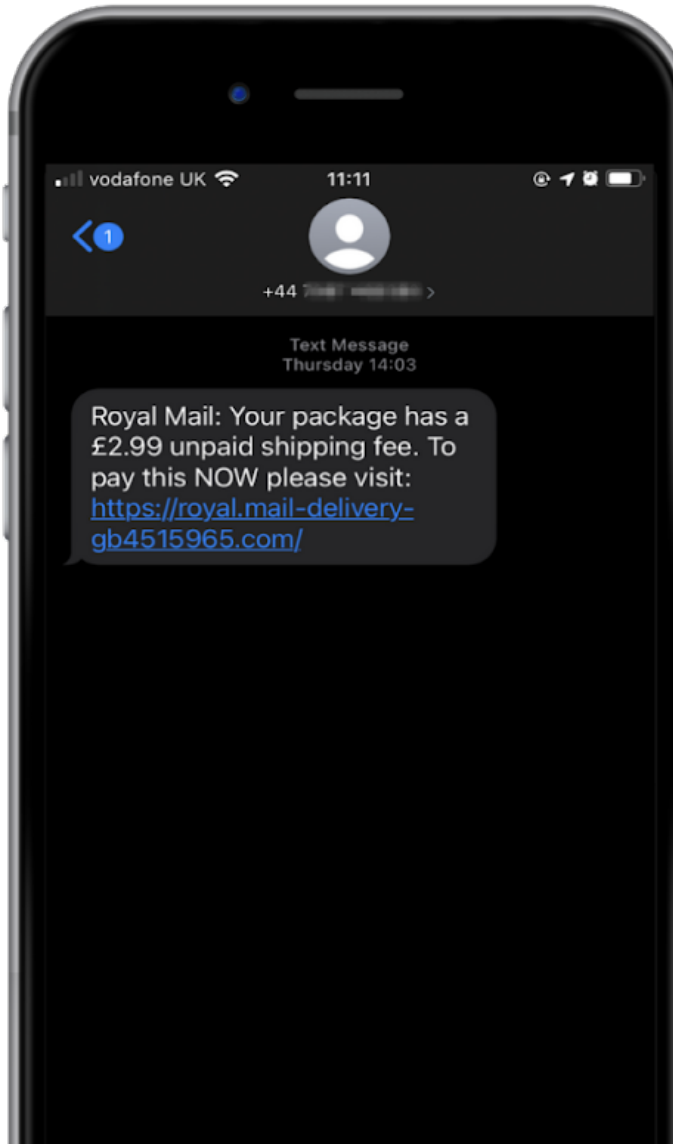
If mobile phishing can lead to so many data disasters, why aren't businesses doing more

There are 4 myths that could account for why organisations fail to prioritise mobile phishing protection.

Fundamentally, most businesses do not have adequate protection in place, and the dangers of mobile phishing are just not very well understood - with many organisations playing catch-up when it comes to securing mobile endpoints.

Let's de-bunk some common myths around mobile phishing





Mobile Phishing Myth #1

"Our email filters will keep employees safe."

While it's true that good email filters can protect employees to some extent, especially if they use corporate email on their mobile devices, it certainly doesn't protect them from the majority of mobile phishing attacks. In fact, SMS-based phishing (smishing) has sky-rocketed.

Mobile phishing attacks have now overtaken traditional email-based phishing as **the most significant social engineering threat facing organizations worldwide**.

Verizon 2026 Data Breach Investigations Report

In 2022, Twilio suffered a costly breach from an SMS phishing attack. 209 customers and 93 end users of its two-factor authentication app had their accounts impacted by the attack.

Phishing websites or credential-stealing malware can be sent through SMS, social media, chat and messaging services, compromised apps, and even advertising networks like Google.

Text Message
Today 13:33

Your DPD package has an unpaid shipping fee. Pay this NOW at pay-delivery.com

Text Message
Today 13:33

HSBC: You've added a new payee. If this was not you, review securely here



Mobile Phishing Myth #2

"Our MDM protects us against phishing."

MDM doesn't detect – it manages.

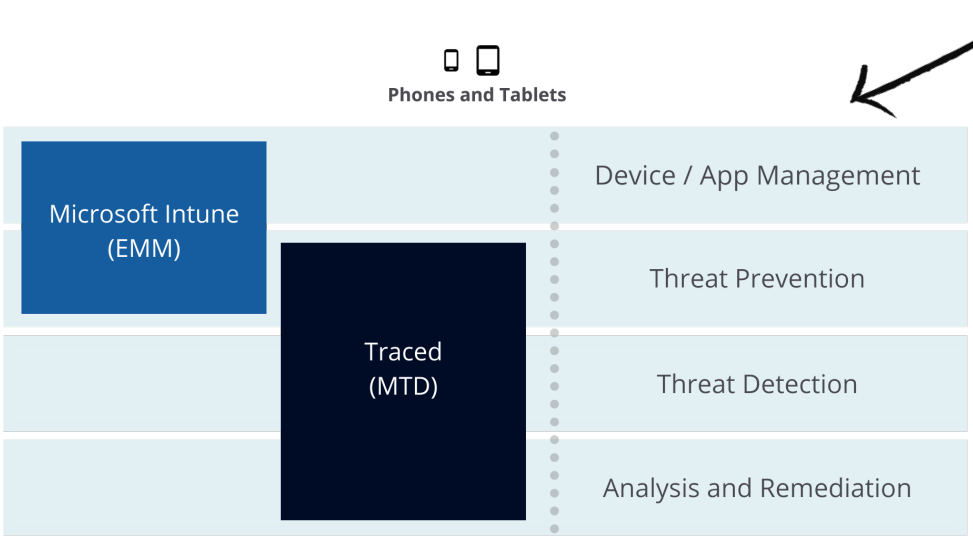
Enterprise Mobility Management or Mobile Device Management solutions are designed specifically for *managing* mobile devices.

As part of managing your organisation's devices, it can deploy policies, apps, and configuration to them.

What these solutions don't do is provide any threat detection, analysis or remediation capabilities out of the box.

So your MDM, MAM or EMM typically doesn't block phishing links or spot malware.

Here's an example of how a popular EMM, Microsoft Intune, fits in with MTD



Mobile Phishing Myth #3

"My phone's built-in security is enough to protect me."

Mobile phishing is an OS-agnostic problem.

In fact, more phishing attacks take place on iOS than on Android devices.

Because phishing links can come via many different methods - text message, email, WhatsApp messages, social posts, apps... there is very little your phone's security settings can do to protect you from attack. Phishing links look just like any other link on the face of it, and the web page they open can be innocuous enough.



63% of phishing attacks take place on iOS devices, not Android.

You give your personal information away on that web page and that data is sent to an attacker - and there are no consistent clues that tell your phone, "*this is a phishing link*."

Mobile Phishing Myth #4

"Mobile phishing isn't a business issue, it's a personal one."

Cybercriminals use phishing to steal credentials, drop malware and gain unauthorised access.

Whether those phishing attacks are sent via mobile-only methods (such as SMS or WhatsApp), or by traditionally desktop-focused methods (like email or social media) they have the same outcome.

Even organisations who have splashed out on corporate phones for employee use aren't immune.

The fact is that we are all vulnerable to falling for a phish and it puts both our personal and business data at risk.

Malware that spreads via SMS has the potential to send thousands of text messages per day from infected devices and racking up eye-watering bills.

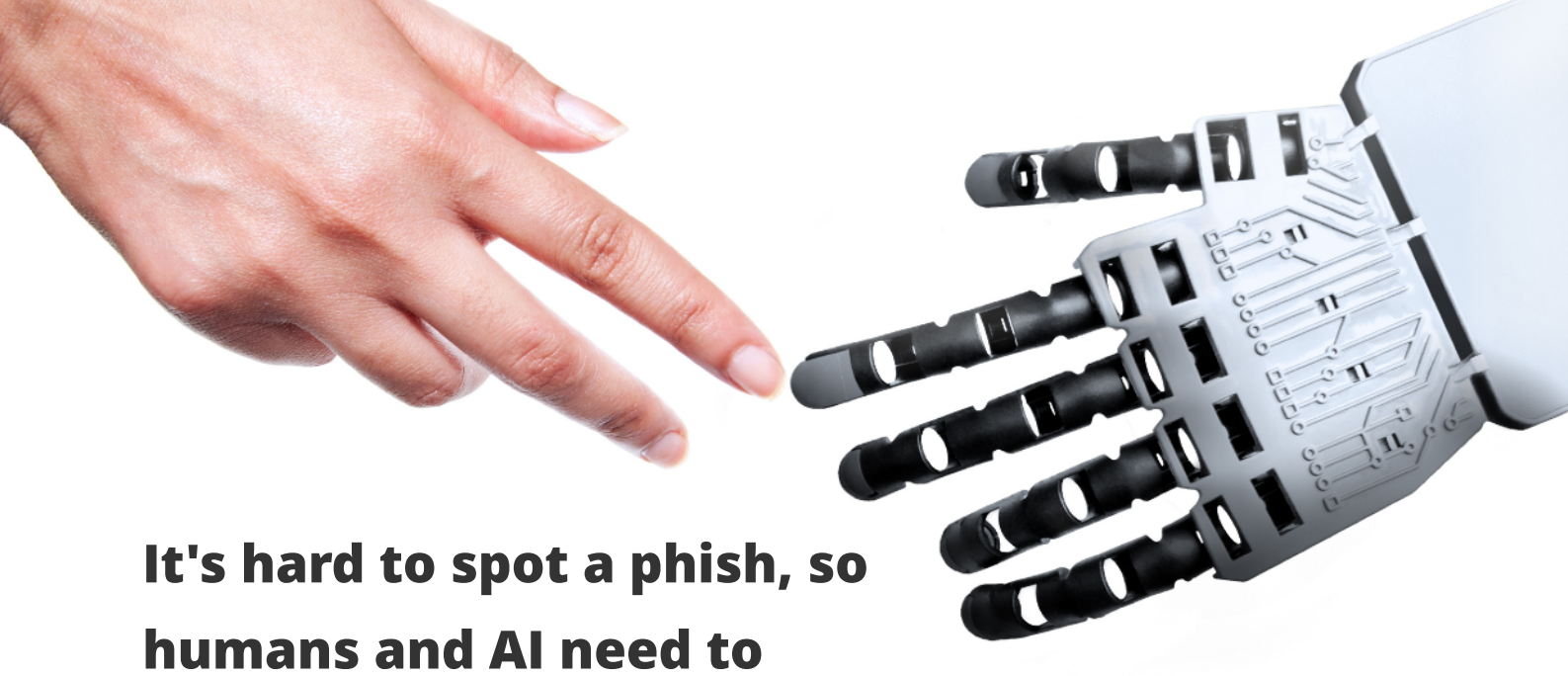
Attackers could land themselves a set of bank credentials for a company account, or login details for business platforms like Office 365 or Google Workspace.

This could also be used for Whaling within an organisation through BEC or WhatsApp by masquerading as the CEO.

Banking Trojans like Trickbot, Eventbot and Anubis are spread via mobile phishing and could be used drop ransomware on the network.

Trickbot, as an example, gathers users' mobile numbers to contact and dupe them into installing a malware Android app that steals their 2FA tokens.

So even if you've set up 2FA on business systems, your employees' phones can pass codes over to an attacker.



It's hard to spot a phish, so humans and AI need to work together

When phishing happens on a mobile phone, it can be a lot harder to spot. Although humans are cleverly wired to detect that "fishy" smell (pun intended)...

> ***Is that person being too pushy?***
>
> ***Was I expecting that message?***
>
> ***Would that company really ask me for that sort of personal information?***

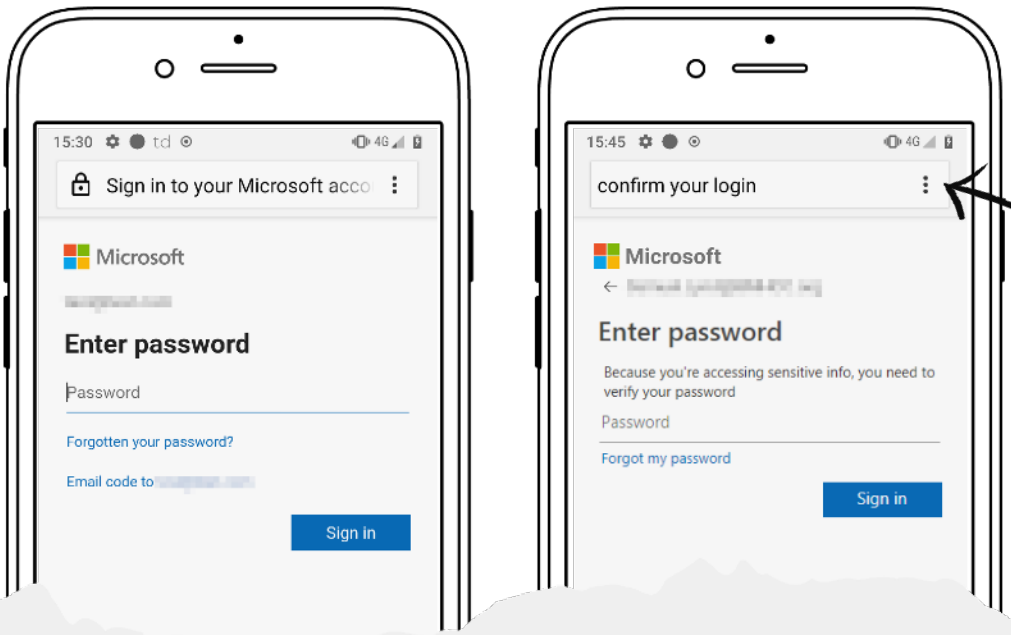
It gives us an edge over technology, it's actually really hard to spot a phish on a mobile phone. ***Why?***

- It catches you off-guard when you're distracted.
- It arrives on tiny screens.
- It targets devices that aren't protected by your company network.

Cyber Criminals are using AI to build their phishing attacks for optimised attack success rates. Coaching staff on how to spot suspect emails is very useful when applied to desktops. Unfortunately, the same strategies don't apply to mobiles, so it's important to add in a layer of defense that uses AI to defend against phishing as Cyber Criminals evolve their attacks.

AI-automated phishing emails achieved 54% click-through rates

Microsoft Digital Defense Report 2025



Note the browser bar. The phish (on the right) obscures the URL with a message, similar to the one the real Microsoft page has.

Phishers are increasingly using techniques which are better suited for targeting mobile users, as mobile users have fewer tools at their disposal to identify phishing links and are more likely to click on them.

Microsoft is the single most impersonated brand in Q2 2026, appearing in 23% of all brand phishing attempts

Brand Phishing Report Q2 2026, Check Point

Combining user education with the Trustd Mobile on-device, AI-powered phishing detection engine is crucial. The threat engine spots the repeating characteristics of a phish, blocking malicious content before it opens on the device, even if the user clicks the phishing link. This advanced anti-phishing technology means that even never-seen-before phishing links can be identified, instead of relying solely on out-dated lists of known phishing URLs.

The future of phishing

Attackers will chase the large payouts they can score from ransomware, using the intelligence they gather from mass phishing campaigns.

We expect to see an increase in targetted phishing as criminals attempt to evade phishing detection models and chase the large payouts from ransomware, rather than lots of small financial wins from mass email phishing.

Along these lines, mobile phishing in all its forms will become a greater concern for businesses, as attackers exploit the various ways that make phishing harder to spot on mobile devices. As business data is increasingly stored and accessed from mobile devices, it makes employees a more desirable target for phishers, and attacks will evolve to be more sophisticated, more prolific and more effective.



AI-driven anti-phishing on mobile devices learns to spot new phishing links to keep up with evolving attacks, but user education needs to go hand-in-glove with on-device protection.

About Trustd MTD

Trustd MTD is the market leading, AI-powered Mobile Threat Defence that saves organisations' time and money by protecting them against costly data and compliance breaches from mobiles, without impacting users.

Find out more at https://trustdmobile.app/

© 2026 Traced Ltd. All rights reserved.