

SPONSORED 

# Simon Community ensures maximum security for its workers' mobile devices

With security threats rising and an increasingly mobile workforce, the Dublin Simon Community needed a way to protect its staff from online scams, malware and phishing threats while enabling them to carry out their vital work during a busy time

🕒 Tue, Nov 24, 2020, 09:00 | Updated: Tue, Nov 24, 2020, 09:20

Sponsored by  
**Three Ireland**

## ... The challenge

For more than 50 years, the Dublin Simon Community has provided help and support to those who are sleeping rough on the streets, and those at risk of homelessness. Having started by providing soup to the homeless, the charity has gone on to expand the emergency and outreach services it provides to include housing, health and advice, addiction treatment and recovery. As well as the residential services like emergency shelters and long-term housing, the Simon Community's outreach work aims to sustain tenancy and keep people in homes, and helps to find accommodation for people who are sleeping rough. In addition, it now operates across not just Dublin but also Kildare, Wicklow, Meath, Louth, Cavan and Monaghan.

For these reasons, mobile devices are an essential part of the Dublin Simon Community's work. Many of its key employees are not based in the office but are out in the community where they rely on their phones such as when they're on a site visit and they need to record case details, take photos or share information with colleagues. The charity's tenancy management and property management teams also visit homes throughout the Leinster area, so mobiles are essential for them. Senior management use their phones extensively for emails, scheduling, and calls. Other times, mobiles are vital for awareness-raising and engaging with the public through social media.

Earlier this year, with the homeless problem worsening the charity was naturally busy, and on top of this, it noticed a surge in cybercrime activity. The leadership team had been targeted by SMS scams on their mobiles more often. There was also a spike in phishing messages appearing to come from banks, along with fraudulent emails that were designed to trick people into sending money to fake accounts.

## The solution

Charities are a favoured target for cybercriminals, so the Simon Community has always invested in good security, including encryption for its mobile devices. However, this didn't protect against threats outside the organisation's own protected network. "Covid-19 was the perfect timing for fraud – suddenly you had many more people working remotely, and they no longer had office firewalls and virtual private networks to protect them," says Martin Hannigan, Simon's Head of Finance and Corporate Services. "We could see the vulnerabilities we had on mobiles and our virus checkers and firewalls were showing an increase in potential attacks on desktops and laptops. You can't hover over an email address on a mobile to see if it's genuine like you can on a laptop. That was always a vulnerability, so to have that extra layer of security is essential."

The Simon Community worked with the security consultancy CWSI, which proposed using 3Mobile Protect, a solution based on Corrata's mobile security technology, in partnership with Simon's mobile provider Three. In phase one of the project, 10 of the charity's senior leadership team had the solution installed on their mobiles, and it was rolled out to the remaining employee mobiles in phase two. The security tool detects and blocks malware, removing the risk that someone could inadvertently download a file that causes their device to stop working or steals its data. The tool also blocks access to phishing sites, malware download servers, and unapproved content and services.

## The benefits

Security improved immediately and noticeably since Simon installed 3Mobile Protect, as it blocks any attempt to connect to a malicious site. At a busy time like the Covid-19 period, this meant that Simon Community staff saved valuable time

by not having to manage the many threats that can affect mobiles, including social media scams, SMS fraud, or malicious apps.

The 3Mobile Protect security solution generates very granular data showing the types of threats against the Simon Community, and attack patterns over time. Its IT team can see the security of their devices all from a single portal. “It’s prevented potential attacks that we never would have been aware of before,” says Martin.

Deploying the technology was easy and fast, needing a single 20-minute call followed by some simple installation. “It’s seamless: in a couple of clicks, you download the app, it’s on your phone, with no adverse effect on the phone’s performance – that’s one of the big advantages for our users,” he adds.

By default, any new employee joining the Simon Community will have enhanced security preinstalled on their mobile device. The Simon Community now plans to use the solution for managing and reporting on its mobile device usage, which will create a culture of ongoing best practice and safety for its users as well as a stronger audit trail which helps its compliance efforts.

The Simon Community now has maximum security across all devices as standard. “You can never have too much security,” says Martin. Most importantly of all, this means its team can focus on their efforts on supporting the homeless

*To find out more about mobile security and 3Mobile protect solution, watch our recorded webinar [here](#)*