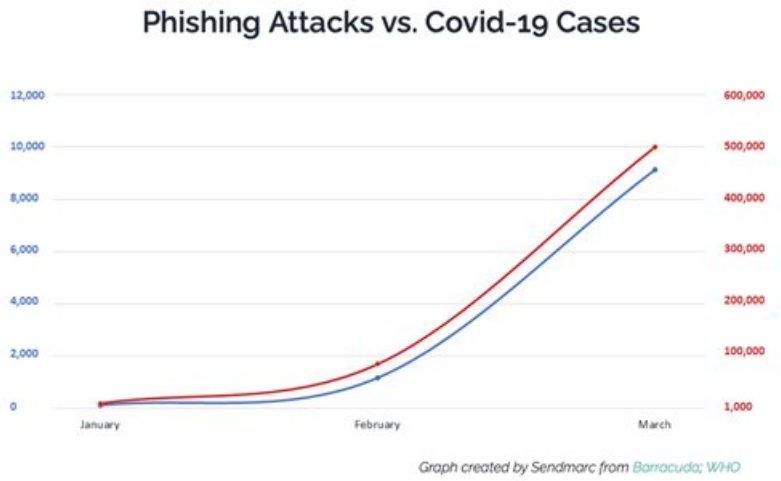
Cyberattacks on healthcare responders increase

As if Covid-19 wasn't enough of a crisis, the number of cyberattacks on frontline healthcare responders have surged at the same time as the global pandemic, trending upwards almost entirely in line with case numbers.

By March 2020, phishing emails had spiked by over 600% since the start of the Covid-19 global pandemic in February, as cyber criminals looked to capitalise on the fear and uncertainty generated by the virus. One third of these attacks used impersonation of a known brand as a tactic to steal money and data, or to deploy a virus or ransomware.

When comparing the number of phishing attacks and Covid-19 infections globally between January and March of this year, the rate of growth in phishing attacks correlates almost perfectly with the rate of increase in Covid-19 infections:



While these attacks have been seen mostly by healthcare institutions around the world, the World Health Organisation (WHO) has also become a target since the pandemic began, reporting a fivefold increase in the number of cyber attacks compared to the same period last year. These attacks were directed at both the WHO's staff and the public at large.

Closer to home, South Africa's Life Hospital Group suffered a cyber attack in June that affected its admissions systems, business processing systems and email servers. As these attacks increase, South Africa's already stretched healthcare system faces even more pressure.

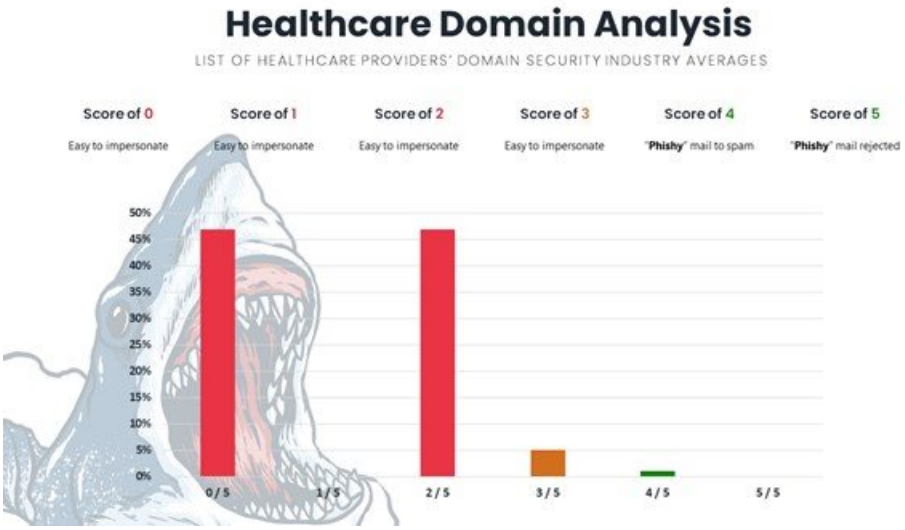
As part of their advice for preventing these attacks on healthcare providers, Interpol issued a statement in April advising staff not to open emails from untrusted sources, nor to click links in emails they were not expecting to receive.

Sophisticated cyberattacks

However, in recent years, criminals have become so sophisticated that they are becoming experts at impersonating genuine emails that it's become very difficult for the user to decide what is safe and what is dangerous. A more effective way to deal with these kinds of cyberattacks is to leverage technology as much as possible before expecting an employee to make a decision about a particular email. One of the most effective ways to do this is to make sure that domains are DMARC compliant.

"DMARC is a global cybersecurity standard that was designed to stop a cyber criminal from being able to impersonate corporate email addresses and thereby commit attacks know as spoofing and phishing," says Sacha Matulovich, CSO and co-founder of DMARC security company Sendmarc.

In order to gauge how vulnerable are South African healthcare institution domains are to phishing attacks, Sendmarc recently conducted research into 219 domains used for email by hospitals, clinics, laboratories, treatment and medical practitioners. The results are shown in the graph below:



Out of the total South African healthcare domains analysed, almost all of them scored three or below on the Sendmarc Safety Score, meaning that their domains are very easy to impersonate and are heavily at risk of a phishing attack.

"It's clear from our research that South Africa's healthcare sector seems woefully ill-equipped to deal with this increase in cyberattacks," says Matulovich. In response, the company will launch a new programme that aims to help a wide cross-section of frontline responders – from hospitals and clinics to laboratories and ambulance services – become DMARC compliant. The programme will be launched mid-September, when further details will be made available.

"Our goal is to help relieve the strain, confusion and threat of loss from healthcare providers who may be vulnerable to cyberattacks at a time when cybersecurity is the last thing on their minds," says Matulovich.