



THE INCREASING RISKS OF PHISHING ATTACKS AND STRATEGIES TO MITIGATE THEM



PAPER BY KIERAN FROST - COO SENDMARC

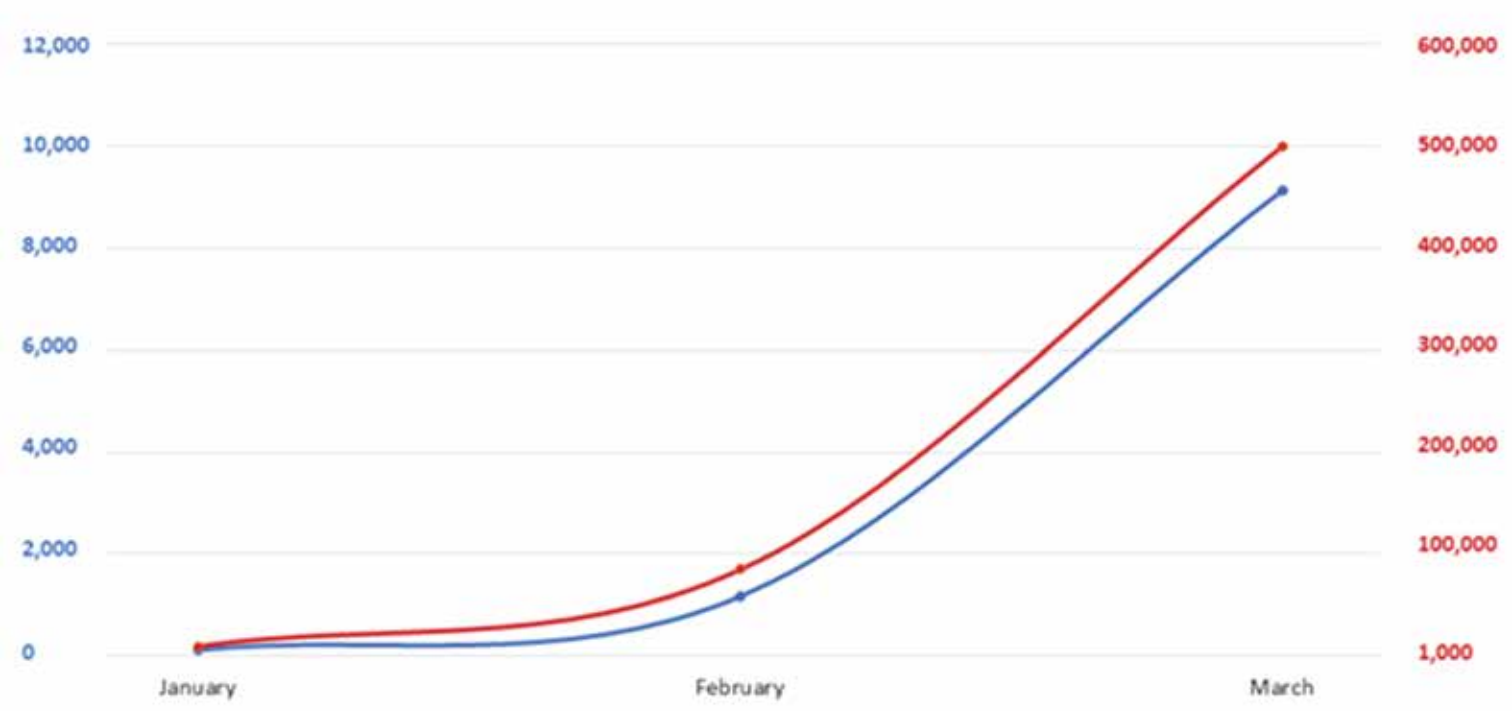


There is the old saying that goes, “When you love what you do, you have never had to work a day in your life,” bWhether you’re an SME or a large multinational company, the risks of being victim to a phishing attack have never been higher, as criminals – and technology – become more sophisticated.

In 2018, the McAfee Economic Impact of Cybercrime Report found that the estimated cost of cybercrime was \$600 billion. And years before that, phishing defence company Cofense (formerly PhishMe) found that the vast majority of cybercrimes (91%) start with a phish. That makes sense if one thinks of phishing within the world of cybercrime as being akin to cutting the electric fence surrounding a house that is consequently burgled: if that initial defence is breached, an asset is left open to a wide variety of crimes.

Given the context amid the Covid-19 pandemic, data is emerging of how impersonation fraud has increased over the near-worldwide lockdown period, as “threat actors” began taking advantage global pandemic. Microsoft’s threat intelligence team, for example, reported a global increase in opportunistic phishing attacks since the Covid-19 pandemic began.

In fact, when comparing the number of phishing attacks and Covid-19 infections globally, it becomes evident that the rate of growth in phishing attacks correlates almost perfectly with the rate of increase in Covid-19 infections. The relationship between these two crises is illustrated in the graph below:



But what kind of damages can stem from phishing attacks? Predictably, attackers are usually after money – and they often get it right. One of the starkest examples of this is the case of FACC AG.

FACC AG is a European manufacturing organizations who produces parts for the likes of Airbus and Boeing. In 2016, Security Week reported that the manufacturer had lost \$54 million dollars (almost 10% of their annual revenues) in an attack. The attackers had impersonated the CEO, and emailed instructions for the transfer of funds to take place. This attack also ended up costing the CEO of 17 years his job. Bring this back home, in South Africa, the cost of cybercrime to the public was a staggering R2.2 billion in 2017.

While the financial consequences are enough cause for concern, there can also be other long-term ramifications to your business:

- Brand damage. A phishing attack on your domain can result in severe reputational damage to your brand – even though you had nothing to do with the attack. The example of Experian in 2020 is stark reminder of this.
- Ramifications for executives. If you're an executive in a company who falls victim to such an attack, you may have to go to court, face the media or even lose your job – as was the result in the FACC AG case - as the person who was responsible for the damage that resulted.
- Less room for plausible deniability. When phishing first became a threat several years ago, company executives could claim that there was nothing they could have done to prevent such attacks, as they didn't know the risks. However, this picture is swiftly changing due to increasing adoption of security controls such as DMARC (discussed later) and greater scrutiny of IT security practices in the board room.
- Risks to customers. Protecting your domain against impersonation is not just about your own company security – it's about protecting your customers' data too. Should your domain come under threat, there's a very real chance that your customers could be affected too, which in turn could cause serious damage to your brand. As a corporate citizen, securing your domain is simply the responsible thing to do.

There are a number of responses to mitigate these risks including educating users about the risks of impersonation and taking simple actions like enabling Two Factor Authentication on your platforms of choice. However, one of the most powerful steps you can take is to implement DMARC on your domain.

DMARC – Domain-based Message Authentication, Reporting & Conformance - protects domain owners against impersonation. With a DMARC record in place, only the legitimate sources of email (such as your selected email marketing platform, your everyday email platform and your billing engine) are able to send mail from your environment. Every domain owner can and should know where they stand with regards to DMARC.

While the risks of attack are increasing, so too are the power of the tools at the disposal of good guys – and making it harder to impersonate your domain is a good place to start.



STOP PHISHING IN ITS TRACKS

CONTACT FOR MORE INFO

QUERY@XCONTENT.COM