BIZCOMMUNITY

# Human fallibility remains the weakest link in cybersecurity

By Yash Pillay

19 Jan 2021

If the South African financial industry can learn one thing from Experian's 2020 data breach, it is this: human fallibility is still the weakest link in the fight against cyberattacks.

Photo by Joshua Woroniecki on Unsplash

By using standard social engineering techniques – simply asking the right question at the right time - the 2020 Experian fraudster, posing as a client, gained access to 24 million individual personal records, as well as confidential financial information for almost 800,000 companies.

Similarly, 2020's Twitter data breach saw of hundreds of high-profile accounts breached, similarly achieved with one simple phone call to an unsuspecting technician.

Quite literally, data breaches are becoming a costly illustration of the old axiom 'loose lips sink ships' where manipulating human nature and exploiting human emotion can have dire consequences.

Whether it's in the form of a low-tech phone call and traditional phishing email or a more sophisticated malware and ransomware invasion via non-reputable applications and uncertified websites on unsecured networks, the holes are getting easier to open and the attacks more difficult to spot.

## Health fears and economic uncertainty as phishing bait

As we enter 2021 and continued era of Covid-19 and the remote workforce, cybercriminals are using health fears and economic uncertainty as phishing bait to lure employees at home, where the links between their personal and professional lives are intersecting across multiple electronic devices using unsecure, non-regulation software over often insecure networks.

Companies, particularly within the financial industry where the digital exchange of sensitive financial and personal information has to be vigilantly managed and regulated, must also take a proactive approach to ensure all aspects of IT gatekeeping infrastructure – hardware as well as software - protects their employees at home.

Commissioned by multinational cybersecurity software company Trend Micro, the 2020 Head in the Clouds research report has evaluated how well the remote workforce is mindful of and prepared against potential cyberattacks.

The research sampled 13,214 remote workers across 27 countries and found that while most employees understood the dangers of cyber intrusion and could identify and avoid the trademarks of a typical digital breach attempt, there is a growing concern about bad security practises of employees at home, using less secure personal devices to access corporate data, and vice versa: corporate devices for personal use.

## Running a tight ship, while managing a dispersed fleet

To avoid the next Experian, South African banks, financial institutions and corporations will need to re-evaluate their cybersecurity infrastructure on three fronts, namely: people, policy and technology.

In managing and securing the remote workforce, companies can now no longer define themselves by location alone – outdated policies and obsolete technology cannot cover one building, one office, one department, with a single security blanket.

Constant education and awareness programmes may be effective to a point: It's not only about teaching employees to spot the newest methods and signs of potential breach attempts, but also changing behaviour and creating a culture of accountability for devices – both personal and work-related - and their online habits.

A stronger relationship between the workforce and a company's IT management is vital in determining a stricter yet adaptable usage policy. Employees should always be aware of what exactly is acceptable practise online and what behaviour is considered irresponsible.

Ultimately, even the most sophisticated protection technology and the best online security processes can only be as effective as the culture of informed, accountable employees that the technology has been designed to protect.


### ABOUT THE AUTHOR

Yash Pillay is a sales engineer at Trend Mcro.