Hi Pearce,

You raise an interesting point about how security vs. user friendliness is a trade-off. A obvious instance of this is seen on major banking websites, which use several authentication and authorization measures, including multi-factor authentication and one-time passwords. I also concur completely with the ignorance about cyber security that is prevalent among MSMEs (micro, small, and medium-sized enterprises), which leads me to highlight some of the reasons why MSMEs do this.

As SMEs and startups embrace technology and digitise their operations as part of their development and market relevance strategies, one critical component that is sometimes overlooked is cybersecurity. The primary cause of such a chasm is the widespread erroneous notion that they are too small or insignificant to be a target.

It's important to remember that SMEs and startups operate on a shoestring budget. This does not, however, absolve SMEs from security expenditures. For the majority of SMEs, smart security entails adhering to key principles such as selecting a strong, legitimate IT infrastructure and applications for business, minimising the footprint of critical and confidential data across desktops, laptops, and emails, layering cyber-defense technology into IT systems that manage sensitive data, instilling a culture of "trust but verify," and finally, planning for cyber insurance to cover for financial losses.

**References**

* Bhat, P. (2021). “MSMEs” flawed belief of being too small to be attacked is root cause for ignorance of cyber security’. Financialexpress. Available from: https://www.financialexpress.com/industry/sme/cafe-sme/msme-tech-msmes-flawed-belief-of-being-too-small-to-be-attacked-is-root-cause-for-ignorance-of-cyber-security/2187848/ [Accessed 26 Mar. 2022].
* PTI Ranchi (2021). MSMEs vulnerable to cyber threats with growing digitalisation: Officials. Deccan Herald. Available from: https://www.deccanherald.com/national/msmes-vulnerable-to-cyber-threats-with-growing-digitalisation-officials-1033620.html [Accessed 26 Mar. 2022].