For any organization, continuously strengthening its cybersecurity posture is mandatory — especially in the wake of the recent surge of post-pandemic attacks. However, most cybersecurity strategies tend to focus on automated protection and mitigation, and only rarely look at things from the human angle.

As a matter of fact, the majority of cyberattacks succeed because an employee made some kind of mistake. Even today, the principal attack vectors come from the oldest venues in the world — such as phishing emails, password thefts, and insecure Bring Your Own Device (BYOD) policies.

Techniques Putting You At Risk

1. Social Engineering

Social engineering is a deceptively effective way to steal credentials and gain access in even the most securely protected network. It works by preying on the most vulnerable people to fraudulently extract or extort information, and it's mind-bogglingly effective: Social engineering reached over $250 million in damage just in 2020.

2. Phishing-As-A-Service Solutions

Given how advanced natural language processing software has become, spotting a fake email is not as simple and immediate as it was before. And while they may look like a trivial threat, 90% of cyberattacks originate from email, causing nearly $6 trillion of damages in 2021 alone.

3. Convincing Forgeries

It's no secret that cybercrime spiked in the COVID-19 era. This trend continued as vaccines became widely available and cybercriminals began selling fake COVID-19 vaccination certificates online.

No cybersecurity perimeter will ever be 100% safe, regardless of the technologies employed. Dangerous online bandits will keep lurking in the darkest corners of the internet, innovating new ways to lure those who lack the awareness to identify their fraudulent approaches immediately.

No matter how far technology can go, we still remain just humans, prone to mistakes and failure. So, it's vital to remain vigilant and fight back against cyberattack using equally sophisticated approaches.