Submission to the first substantive session of the UN Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025)
(December 2021)

Contribution by KnowBe4

On the occasion of the first substantive session of the second Open-ended Working Group (OEWG II) on security of and in the use of information and communications technologies (2021-2025), KnowBe4 wishes to share its views on the topics under consideration by the OEWG, as mandated by General Assembly resolution 75/240 and contained in the OEWG's agenda (A/AC.292/2021/1).

Informed by the OEWG Chairperson Ambassador Burhan Gafoor and his intention for the OEWG to be a platform for action, KnowBe4 highlights specific and concrete views for the OEWG's consideration in relation to the human element within the cybersecurity threat landscape of information and communication technologies.

In our capacity as a global provider of cybersecurity awareness education and as security culture advocates, we concur with industry research findings which state that that social engineering attacks are on the rise and are the biggest instigator of the majority of cyber-attacks. Social engineering bypasses technical defenses and targets the human as a means to compromise systems. In the past year alone, ransomware has become a disruptive form of attack affecting business continuity and threatening economic prosperity. This has prompted military leaders in some countries to publicly recognize the threat ransomware poses and their willingness to use military force to respond.

As an international leader in the field of human cybersecurity, security awareness education and security culture we would like to offer the following views in relation to item (b) and (g) in the discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240:

> **(b) To consider initiatives of States aimed at ensuring security in the use of information and communications technologies**
> Our view is that cybersecurity awareness is not a technology skill but a life skill. One that governments should actively incorporate into public school curriculum from elementary through high school. Separately from public school education, States should consider regulations or standards relating to cybersecurity education across industries that encourage continuous education, testing and behavioral interventions in support of social norms that build cyber resilience.

(g) Capacity-building

Our view is that as the digital economies of the world grow, economic prosperity will be even more intertwined with cybersecurity where humans are at the digital frontline. Cybersecurity capacity building at a national level will be paramount to cyber resilience in the face of a growing cyber threat landscape (eg: smart cities, smart industries, digital health etc). As such, cyber security education in the pursuit of security culture should be seen as a vital pillar for cyber capacity building and national resilience in our information and communications technology infrastructure in the modern age.

Proposed Action for the OEWG:

We believe that cybersecurity education at a national level will help manage and reduce successful social engineering attacks and protect individuals, organizations, businesses, intellectual property, and critical infrastructure.

We propose that the OEWG leverage its non-governmental stakeholders to determine educational cybersecurity topics that States can consider as part of their national public education system K-12 as well as higher education institutions and industry level education.

Knowbe4 is ready to assist and support conversations with States and other non-State Stakeholders of the OEWG to bolster global cybersecurity awareness and strengthen our global security culture to prevent and mitigate cyber attacks.

About KnowBe4

KnowBe4 is the world's largest security awareness and simulated phishing provider helping businesses, governments and critical infrastructures manage social engineering threats. Operating on every continent and in 35 languages KnowBe4 is unrivaled in its understanding of the global human cybersecurity landscape and the content in its security awareness training library. Learn more at www.knowbe4.com