Submission to the third substantive session of the UN Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025)
(July 21, 2022)

Submission by KnowBe4

On the occasion of the informal dialogue of the third substantive session of the Open-ended Working Group (OEWG) on the security of and in the use of information and communications technologies, KnowBe4 wishes to respond to the OEWG Chair’s letter on the 13th of July, 2022 inviting stakeholders to share ideas and best practices on the topic of capacity building. KnowBe4’s written submission specifically addresses the following portion of the Chair’s letter:

“In particular, at this informal dialogue, I invite stakeholders to share your thoughts and ideas on best practices and lessons learnt with regard to stakeholder involvement in ICT capacity-building initiatives.”

Verizon’s 2022 Data Breach Investigations Report states that “the human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse or simply error, people continue to play a very large role in incidents and breaches alike.”

Findings from the KnowBe4 2022 Phishing by Industry Benchmarking Report

As the world’s largest security awareness training and simulated phishing platform, KnowBe4 has helped tens of thousands of organizations across industries reduce their human risk vulnerability. Each year KnowBe4 releases its annual study reporting the state of Phishing which highlights how susceptible each industry is to phishing attacks – this is represented in their Phish-prone™ Percentage (PPP). With the world’s largest data set across industries and continents on phishing, KnowBe4 finds education to be a key contributor in reducing human risk. The graphic below outlines the methodology and the data used for this study:
The report’s findings show that there are several key critical infrastructures that have a notably higher phish prone percentage. Out of the 19 industries included in this study, the industries that have the highest susceptibility to falling victim to human related cyber attacks are: education, banking, healthcare, energy and utilities.

Who’s at Risk?
The top three industries by organization size

<table>
<thead>
<tr>
<th>SMALL 1-249</th>
<th>MEDIUM 250-999</th>
<th>LARGE 1,000+</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.7% Education</td>
<td>39.4% Hospitality</td>
<td>52.3% Insurance</td>
</tr>
<tr>
<td>32.5% Healthcare &amp; Pharmaceuticals</td>
<td>36.6% Healthcare &amp; Pharmaceuticals</td>
<td>52.2% Consulting</td>
</tr>
<tr>
<td>31.5% Retail &amp; Wholesale</td>
<td>34% Energy &amp; Utilities</td>
<td>50.9% Energy &amp; Utilities</td>
</tr>
</tbody>
</table>
Best Practices: Mitigate and Manage Human Risk to ICTs

Information Communication Technologies (ICTs) are an integral component of the international economy. This reliance on ICTs continues to be criminally exploited both from the human layer as well as the technology layer. This human risk is primarily exploited through social engineering attack vectors and due to the shortage of skilled labor and the increasing number of cyber-crime incidents, organizations need to focus on people as a critical security layer.

Best practices to reduce human risk involve:
- Investing in security awareness programs to enable people to make better security decisions to train users on an ongoing basis to make all users aware of the latest threat landscape.
- Actively building security culture.
- Education on social engineering and the latest in cyber-attacks.
- Simulated phishing campaigns.

The findings in the KnowBe4 2022 Phishing by Industry Benchmarking Report demonstrates that education can make a difference in an organization’s human risk posture by improving cybersecurity literacy. It also supports other studies that identify the link between education and lower incidents of successful social engineering attacks.

In support of this research, lessons learned and the data KnowBe4 has offered to donate a curated selection of its education to all Member States for use in schools to help educate school age children. As non-governmental stakeholders we believe that this ICT capacity-building measure can help prevent and mitigate the human risk and curb the success of cyber attacks.