The UN Office of Disarmament has established the Open-Ended Working Group on security of and in the use of information and communications technologies (ICT) 2021-2025 to address the challenges and opportunities of cyberspace. As a member of the committee, SafePC Solutions, in collaboration with Praxis AI, has developed a Cybersecurity Awareness Training Program utilizing a learning experience platform (LXP).

The Praxis AI learning experience platform (LXP) is an AI-powered online learning platform that allows researchers and educators to design, implement, and evaluate various learning interventions in online environments. The LXP integrates data collection, analysis, and feedback mechanisms to enable rapid iteration and improvement of learning outcomes. The LXP can be used for various purposes, such as testing hypotheses about learning processes, optimizing instructional strategies, transferring workforce skills, personalizing learning paths, and enhancing learner engagement and motivation.

The training aims to help participants learn how to defend themselves and their organizations from cyber threats, and to promote regional, cross-regional, and inter-organizational collaboration and skilling. I suggest that we review the training program during our Mapping exercise and collect feedback from committee members and stakeholders on how to improve the effectiveness of the training to build capacity, and furthermore this will address the main challenges in the ICT industry which is the lack of cybersecurity skills which further impacts capacity building.

Overview of the Cybersecurity Awareness Training Program

Cybersecurity is a vital aspect of the digital world, as it protects both individuals and organizations from malicious attacks that can compromise their data, privacy, and reputation. To achieve a high level of cybersecurity, there are some foundational technologies that should be implemented and followed. These include:

- **Multi-factor authentication (MFA):** This is a method of verifying the identity of a user by requiring more than one piece of evidence, such as a password, a code sent to a phone, or a biometric scan. MFA adds an extra layer of security and makes it harder for hackers to access accounts.

- **Password management rules:** These are guidelines for creating and maintaining strong passwords that are hard to guess or crack. Some of the rules are using a combination of letters, numbers, and symbols; avoiding common words or phrases; changing passwords regularly; and not reusing passwords for different accounts.

- **Password manager tools:** These are software applications that store and manage passwords in a secure and encrypted way. They can generate random and complex passwords, autofill them on websites, and sync them across devices. Password manager tools can help users follow the password management rules and reduce the risk of forgetting or losing passwords.

- **Software updates:** These are patches or improvements that are released by software developers to fix bugs, enhance features, or address security vulnerabilities. Software updates can prevent hackers from exploiting known flaws or weaknesses in the software and improve the performance and functionality of the system.

- **Email phishing:** This is a type of cyberattack that involves sending fraudulent emails that appear to come from legitimate sources, such as banks, government agencies, or trusted contacts. The emails often contain links or attachments that can infect the device with malware or direct the user to a fake website that can steal their personal or financial information. Email phishing can be avoided by checking the sender's address, the subject line, the content, and the links before opening or clicking on anything suspicious.

- **AI tools:** These are technologies that use artificial intelligence (AI) to perform tasks that normally require human intelligence, such as analyzing data, detecting patterns, or making decisions. AI tools can help improve cybersecurity by automating processes, enhancing detection capabilities, or providing recommendations. However, AI tools also pose some challenges and risks, such as ethical issues, bias, or misuse. Therefore, users should be aware of the limitations and implications of AI tools and use them appropriately and responsibly.