CybersCool Defcon Inc

Cybersecurity Essentials Workshop Syllabus

About the Workshop

The Cybersecurity Essentials Workshop at CybersCool Defcon Inc. powered by Cybint, is an 8-hour live training program designed to tackle human error by helping learners to develop advanced understanding and skills to protect themselves and their organization against the most common cyber threats .

This workshop covers the fundamental best practices in cybersecurity and is recommended for all non-technical roles in an organization.

Workshop Syllabus

INTRODUCTION TO CYBERSECURITY

In the first session, learners will be introduced to the world of cybersecurity. They will cover what exactly cybersecurity is, basic terminology, and why cybersecurity so important to the world today. They will also learn about the most famous cyber-attacks.

ACCOUNTS & CREDENTIALS SECURITY

One of the most common elements linking cyber-attacks is compromised or weak credentials. In this session, participants will learn different ways hackers can acquire their passwords, and what to do if their accounts have been compromised. They will also learn how to prevent such attacks including best protection methods and password management, and be introduced to tools for testing and creating strong passwords.

REMOTE SECURITY: WI-FI & VPN

As an increasing amount of time is spent outside of the office, workers must be aware of the main risks that arise when using public and non-protected Wi-Fi networks. In this session, they will learn the difference between private and public Wi-Fi networks, what a VPN is and how to use it, and how to browse safely in remote environments.

SOCIAL ENGINEERING

One of the most common methods for carrying out cyber-attacks is “brain hacking,” also known as social engineering. In this session, participants will learn how hackers take advantage of “human-based vulnerabilities”. It will cover what social engineering is, the different types of attacks that can leverage social engineering, such as phishing or vishing, and most importantly, how to detect social engineering attempts and prevent future breaches.

MOBILE SECURITY

Mobile phones are an essential part of modern lives, and usually contain sensitive private information, such as photos, browsing history, text messages, and confidential business information such as emails, documents, access permission and more. In this session, participants will learn how to minimize the risk of an attack on their mobile device and understand basic security principles for mobile applications.

Online Assessment

At the end of the day learners will be asked to complete a short online assessment covering the main topics from the workshop. The assessment contains 10 multiple choice questions and will take approximately 30 minutes to complete. Once finished, learners will receive a Certificate of Completion.