OLINKO
CONNECTING BUSINESS & IT

PROPOSAL

A cybersecurity awareness program for end users that consists of 5 steps, in which we put people at the centre and integrate the approach of change management.

Step 1:

We start out with an analysis of employees' current maturity in terms of cybersecurity. What is the employees' knowledge of phishing, do they recognize cybercrime, and do they know how to stay cyber-secure?

We engage the ICT department and help them to use ***the Attack Simulation Training** proposed in their Office 365 tenant.
This tool provides in an efficient manner how to conduct a phishing campaign, we identify together how we will also use the platform to go to the next level: spear phishing.
The tool provides comprehensive reporting that allows us to pinpoint the aspects that need to be addressed for improvement.

We then organize a workshop with different stakeholders within the organization to identify the concrete needs and define the approach. We will also agree on how to deal with new joiners and preferably include the topic in the onboarding process.
This results in an action plan with various milestones that we can implement immediately.

Step 2:

Initiating the roll-out of the action plan with the aim of creating the necessary awareness so that employees understand what is expected of them and why cybersecurity is a strategic priority for the organization. This message is preferably delivered by an executive-level sponsor. We provide the scripts and can support the client in terms of communication, this is agreed beforehand in the workshop (step 1).

Step 3*:

We work on raising awareness among employees so that they are aware of the various risks present and the role they themselves play
We follow the different milestones of the action plan we outlined in step 1. These can include thematic training sessions, vishing simulations, an e-learning tool (also provided by the Office 365 MDO Plan 2 package or Microsoft Office 365 A5 |E5|F5 and G5 Security tenants), tests using social engineering such as USB dropping, etc.

Step 4:

In between, we measure effectiveness among employees by organizing a survey and adjust the program where necessary.

Step 5:

After a minimum of 1 year of following the program and achieving the predefined KPIs (will be agreed during the workshop), employees will receive a certificate stating that they have sufficient professional knowledge in the field of cybersecurity.

Through our fellow Cronos Partners, further consultancy, support, training and even reconfiguration of systems can be provided, these are optional.

Price for this package:
2500€ including maturity measurement*, workshop, survey and certificate.

***Price does not include step 3.**