Cyber Guru Training

Communication Plan
Cyber Guru

Summary

1. Preamble

This document provides general guidelines for implementing the entire communication plan for launching the Cybersecurity Awareness programme with the two training programmes Cyber Guru Awareness and Cyber Guru Channel.

The Cyber Guru platform will send communications to all participants registered on the platform via an **automated Student Caring system**. The **first communication** will be sent on the fixed date of the **programme launch** and will contain the credentials to access the platform.

In the months following the launch, participants will always be notified by the same automatic Student Caring system when **new modules (one per month) are available** on the platform.

In addition to the automated Student Caring system that underpins the platform, it is recommended to design and link an **internal company communication plan** that would anticipate and promote the launch of Cyber Guru's Cybersecurity Awareness programme to senior management and all employees.

It is also important to establish internal company communication channels, such as the company intranet (with a page dedicated to the launch of the Cybersecurity Awareness programme) or news.

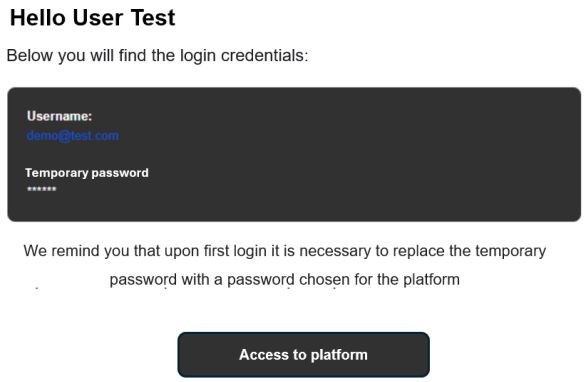
2. Cyber Guru School automated communications

Within the Cyber Guru platform, there is an automated Student Caring system that consists of sending:

- **an initial email launching** the programme on the GO LIVE date agreed between the parties;
- an email sent by Student Caring **in the months following the launch**, notifying the user that the new module is available on the platform.

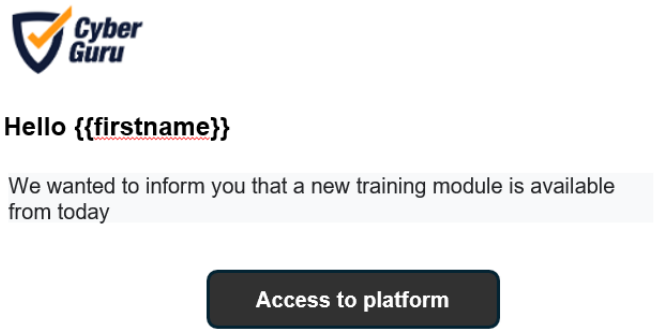
2.1 Cyber Guru communications text launch for the Cyber Security Awareness programme

The wording of the email that will be sent to all users registered on the platform on the fixed go live date of the Cybersecurity Awareness programme, is shown below.



2.2 Cyber Guru Student Caring Communications

Student Caring communications will be issued in the **months following** the launch when each new module is activated.



3. Internal Communication Plan Suggestions

Some tips for managing the **internal communication plan** that we recommend **prior to the launch of the automated communications sent** by the Cyber Guru platform can be read below.

There are two examples of types of communication to:

- senior figures;

- all employees.

3.1 Example of the communication addressed to Senior Figures

Dear [Directors],

In collaboration with the **Division/Area/Department** [indicate the Division/Area/Department promoting the initiative] a [**training programme**] [training course] [training pathway] [an immersive journey], through the **Cyber Guru e-learning platform**, dedicated to the theme of [**Cybersecurity Awareness**] [awareness in the field of Cybersecurity] which, with a commitment of only a few minutes per month, will enable each [user, colleague] to be a custodian of the data they process every day and therefore, protect themselves and the organisation from possible cyberattacks.

The training programme starts [**in the month of...]** or [start date], it will last for [12/24/36 months[1]] and will comprise [12/24/36] training modules and [12/24/36] episodes, each of them focusing on a specific topic.

The **training content** is delivered at a frequency of one per month, and the method of delivery is strictly sequential. As a result, it is necessary to complete one item of content before moving on to the next.

Each module relating to the training component consists of **3 short lessons**, each consisting of a video containing approximately 15 minutes of learning material and, as an alternative, a document reproducing the same content as the video in a text format.

The **3 lessons** within a module are arranged according to the following pattern:

- The first lesson focuses on basic knowledge; it encourages an awareness of the topic at hand, providing the necessary cognitive elements for understanding the risk;
- The second lesson is one of "readiness", enabling the conditions to detect threats, even when they present themselves in an unusual and sophisticated form;
- The third lesson is about best practice: it allows for the acquisition of "good practices" in behaviour, which stimulates "responsiveness" and ultimately the ability to act consciously.

In order to progress from one lesson to the next, it is necessary to pass a test made up of four multiple-choice questions. If you answer at least 3 out of 4 questions correctly, the lesson is considered passed.

Each episode of the training component consists of a video containing approximately 5 minutes of content focusing on the main cyber threats.

[1] 12 first-year modules, 24 second-year modules, 36 third-year modules

[Optional] In order to support the participants' involvement, the training path provides for a **so-called "gamification" methodology,** which can be compared in terms of scoring to a virtual championship, whereby the training path allows for an **individual ranking**, which is used to reward the learner in his or her path and, at the same time, to **enhance the ranking by team,** i.e. by the division to which the individual participants belong.

[Optional] All the statistics are provided in **strict compliance with the Privacy and Data Protection Act**. Each participant is only able to view his or her own indicators, in relation to the team to which he or she belongs – their division –and the improvement in the team rankings.

[Optional] The training course is [mandatory] [optional].

[Within the current week] [By next week], with a follow-up email by [*the sender no-reply@cyberguru.eu*] [*of the Cyber Guru Awareness e-learning platform*] **access credentials will be sent to each participant**.

A support service with a dedicated mailbox [**support@cyberguru.eu**] is provided**.**

[Optional] It will be possible to obtain more information on the dedicated Intranet page [indicate the reference link].

We look forward to your participation and remain available for any further information you may require. Kind regards,

HR Team – Communication Team

3.2 Example of communication sent to the entire corporate community

Dear all,

In collaboration with the **Division/Area/Department** [indicate the Division/Area/Department promoting the initiative] a [**training programme**] [training course] [training pathway] [an immersive journey], through the **Cyber Guru e-learning platform**, dedicated to the theme of [**Cybersecurity Awareness**] [awareness in the field of Cybersecurity] which, with a commitment of only a few minutes per month, will enable each of us to be the custodian of the data we process every day and therefore, protect ourselves and the organisation from possible cyberattacks.

The training course starts [in the month of...] or [start date],**and lasts for [12/24/36 months]; it is comprised of [12/24/36] training modules [and 12/24/36 episodes],** each of which is devoted to a specific topic.

The training content is enabled with [**monthly**] frequency and the method of use is strictly sequential. As a result, it is necessary to complete one item of content before moving on to the next.

Each module consists of 3 short lessons, each of which includes a 5-minute piece of video content and, as an alternative, a document that reproduces the same content as the video in a text format. In contrast, the instructive component consists of a short video of about 5 minutes, again on topics related to cybersecurity.

In order to improve the motivational value of the training course, the e-learning platform provides for the awarding of scores for each correct answer given at the end of the training modules, **enabling you to take part in a virtual championship** that allows you to accumulate points within your reference team, represented by

your division.

[All statistics are provided **in full compliance with regulations governing privacy and the protection of personal data**. Each participant can only see their own marks, related to the team they belong to, and **all data is anonymous**.]

[Optional] The training course is [mandatory] [optional].

By the end of the current week, a follow-up email by [the sender no-reply@cyberguru.eu] [of the Cyber Guru Awareness e-learning platform] **will be sent to each participant with access credentials**.

More information can be found on the dedicated Intranet page [indicate searchable reference link].

We look forward to your cooperation in this endeavour. Best regards,

HR Team – Communication Team

3.3 Activation of internal company channels such as company intranet and news

A number of **internal company channels should be activated** to increase the participation and active involvement of all employees and sustain the success of the programme.

Where possible, a dedicated intranet page can be designed where the gamification dynamics included in the platform can also be facilitated and promoted.

3.4 Post GO LIVE communications

After the Cyber Guru training programmes have started, it may be the case that some users may lag behind in ad hoc targeted communications [by senior figures, e.g. CEOs]. An example of a communication that can be used in these specific cases is given below:

Dear colleagues,

Cyberattacks are becoming more and more sophisticated and dangerous. The techniques used by cyber criminals not only jeopardise the security of our organisation, but also your personal safety. For this reason, we at **[company name]** have decided to implement the Cybersecurity Awareness programme, which entails a commitment of just a few minutes per month that will allow you to acquire the right level of awareness in cybersecurity, protecting ourselves and our organisation from possible cyber attacks.

Unfortunately, we are seeing a [low/very low/not completely satisfactory] level of participation in this programme. At present, we have:

xxx colleagues on track – users who have completed all the modules currently available;

xxx colleagues currently making good progress – users who have completed all of the modules currently available except for the current one;

xxx colleagues who are not on track – users who have acquired at least one point, but who are not on track or regular;

xxx inactive colleagues – users who have not acquired any points.

Therefore, there are xxxx inactive colleagues. We ask for [the participation of the entire company population] [all colleagues] to follow the course in its entirety.

Cybersecurity is currently a major threat to companies, and being unable to spot the risks and dangers of the cyber world exposes us to potential disruption of our business operations. Developing a shared knowledge and sharpening the skills needed to recognise danger is crucial.

We are confident that all our colleagues will take part, because the subject of information security is an issue that affects us all.

Best regards,

The texts and references indicated above are suggestions that can be freely modified to suit the style and tone preferred by the company.

Attachment A – Intranet Page Example

Project	**Cybersecurity Awareness Programme Protect yourself and your organisation Behaviour can make a difference**
Programme	From [month] [year], all [company name] staff will be able to take part in the Cybersecurity Awareness training programme in e-learning format, to raise their awareness of the risks of misusing digital technologies and learn how to protect against cyberattacks.
FAQ	The purpose of the course is to involve everyone on the front line, because anyone could become an unsuspecting victim of cybercrime.
Reports	Be a part of the Cybersecurity Awareness programme: with a commitment of just a few minutes per month, you can acquire the skills necessary to gain awareness and be able to defend yourself.
Operating notes	Log in to the platform
Supporting documentation	Taking part in the initiative will be an opportunity to expand your knowledge while having fun and reinforcing partnerships with colleagues

The Project

As part of its cybersecurity expertise, [Name of the Division's sponsor initiative] is proposing a simple and effective way for each individual to recognise potential threats from the cyber world.

Nowadays, it is estimated that a high percentage of computer security incidents originate from some form of human error, and the most commonly detected forms of errors and risky habits include inadequate management of passwords, failure to recognise fraudulent websites, dangerous email attachments and misleading URLs.

The proposal for this programme therefore stems from the awareness that IT security cannot be entrusted to specialists and technical interventions alone, but must also be safeguarded by investing in the human factor.

With this in mind, the Cybersecurity Awareness Programme offers all staff a simple roadmap to develop a high degree of awareness in the use of digital technologies and web browsing.

The course is delivered via an e-learning platform and is structured into 3 levels
over a period of [one year, two years, three years...].

Each level includes modules devoted to specific topics, learning tests, and participation
in a *"gaming"* phase, designed to stimulate and energise the training course.

Participating in the programme is simple: just log in to the platform using the individual credentials sent by email, and follow the video lesson proposed in the module.
A FAQ section is available for clarification on logging into the platform and its operation, or you may ask for help via email.

The programme

The complete training course programme is organised into three levels, which will be offered over the course of
three years.

The content

Each level is organised into 12 modules and 1 episode dedicated to specific topics.
The modules are accessed through the Cyber Guru Awareness e-learning platform.
Each month, new content is released, and all staff are invited to continue their learning.
The method of delivery is sequential, i.e. it is necessary to complete one piece of content before moving on to the next.

Number of lessons per module

Each module is made up of 3 short lessons, each consisting of a few minutes of video content and, as an alternative, a .pdf document containing the same content.
The module's three lessons are organised as follows:

- the first lesson provides a basic knowledge of the subject;
- the second lesson offers further insight and encourages user "readiness" by creating the conditions to recognise threats;
- the third lesson provides examples of best practices and encourages correct behavioural responses.

Comprehension test

To progress from one lesson to the next, it is necessary to pass a test made up of four multiple-choice questions. To pass, you must correctly answer at least three out of four questions. You can take the test more than once; the best result is always taken into account for training assessment the purposes.

Episodes

Each episode is characterised by a specific cyber theme. There is no test upon completion of the episode.
In this case, too, there is a prerequisite structure, which means that it is necessary to complete one episode in order to move on to the next.

The gaming phase

The project includes:

- an **individual gaming** system in which participants accumulate personal scores comprising medals and cups
- a **team gaming** system in which the staff of each [Department ...] forms a team. Each team will have a team leader and will accumulate its score by aggregating those of the individual members.

To learn more about the scoring system and the game in general, consult the Rules.

FAQ