Cyber Guru

Increase the level of cyber security by targeting the human factor

Cyber Security Awareness

WHITE PAPER

Executive Summary

In a public or private organisation, addressing *Cyber Security Awareness* means raising the level of Cyber Security of the entire organisation in terms of protection of critical business data as well as personal data. It is an investment that produces benefits for the organisation and positive repercussions for the private and social dimensions of the individuals.

This type of investment is becoming more and more urgent due to the rapid growth of cybercrime. In recent years there has been what observers are calling a quantum leap in cybercrime, with damages of over 500 billion dollars, a "volume of business" that exceeds traditional crime.

In the analysis of this scenario, a worrying fact emerges, namely that most of the offences can be traced back to the so-called human factor: improper behaviour is the "door opener" for the strategies used by attackers. More than 80% of breaches were caused by mistakes made by individuals acting unaware of the type and quantity of cyber threats.

In order to act knowledgeably it is therefore necessary for users to acquire the cognitive elements that allow them to develop mature attitudes and adopt proper behaviour concerning Cyber risks. Within any public or private organisation, it is therefore necessary to ensure that non-specialist personnel follow a training path that leads them to make increasingly conscientious use of digital technologies, social tools and web resources.

When making an intervention of this magnitude, which affects all employees of an organisation, you must provide a training path with precise characteristics: extremely effective, efficient, and low impact with respect to the productivity of the organisation.

It must be a stimulating and engaging path, and it must not be limited to the theoretical and notional, but must exercise human factors such as attention, readiness and responsiveness, to enable the individual to react correctly even when faced with unknown threats.

The Cyber Guru solution targets non-specialist personnel at public and private organisations. The main purpose is to reduce cyber risk by targeting the human factor through advanced training that develops threat awareness.

To achieve this goal, Cyber Guru combines the Cyber Guru Phishing solution, dedicated to continuous monitoring of corporate population's vulnerability to Phishing, with the Cyber Guru Awareness platform, an advanced system of Cyber Security Awareness computer-based training.

Cyber Guru Awareness is a platform that applies the most modern educational and pedagogical theories, as well as the most current design paradigms, to ensure maximum usability by a highly heterogeneous user base.

The training is structured into 3 training levels. Each level is composed of 12 modules corresponding to a complete and self-contained training cycle.

The quality of Cyber Guru Awareness is ensured by a particularly effective and detail-oriented development and update process. The creation of generally-accessible training, which until recently it was limited to Cyber Security specialists, requires the utmost attention to every element of the process and the use of the most advanced educational methodologies.

Cyber Security Awareness or *Security Awareness* is defined as:

General awareness of Cyber Security risks while interacting with digital technologies and in particular with the Web

Sommario

Executive Summary ***1***

Definition ***4***

The quantum leap of cybercrime ***5***

The human factor in Cyber Security ***6***

The role of training ***7***

Characteristics of the training course ***8***

Methods of delivery ***9***

Cyber Guru ***11***

Cyber Guru Awareness ***11***

- 3 training levels .....
- 3 lessons per module .....
- Learning tests .....
- In-depth resources .....
- Medals .....
- Evaluation test and cups .....
- Ranking .....
- Team organisation and competition .....
- Certificates .....
- Team leaders and supervisors .....
- Statistics and communication .....
- Cyberpedia .....
- Gamification .....
- Features .....

The development process ***16***

- Delivery platform .....
- User Interface .....
- The development process .....

The first level of training ***18***

The second level of training ***21***

The third level of training ***24***

Definition

Cyber Security Awareness (CSA) can be defined as general awareness of the Cyber Security risks while interacting with digital technologies and in particular with the Web.

Increasing the level of CSA of employees through training helps protect the employee in their professional and social spheres, reducing the risk of them becoming the victim of a cyber attack.

In this case, increasing CSA means raising the level of Cyber Security for the entire organisation,

> *When a person's social sphere is redefined as the public or private organisation in which they operate, this level of awareness takes on even greater value. In this context, the unwitting behaviour of a person in their interaction with the digital world can cause serious risks that threaten the very existence of the organisation.*

in terms of the protection of critical corporate data as well as personal data as governed by Privacy laws, not least the new European regulation on the protection of personal data, GDPR.

Considering that personal and professional spheres are increasingly overlapping, driven by the current levels of digital transformation and the importance that tools such as smartphones have assumed in people's daily lives, any action that increases CSA in the individual produces concrete benefits both personally and professionally.

The quantum leap of cybercrime

In recent years, many observers have recorded a so-called "quantum leap" of cybercrime: an unprecedented growth of criminal activities in the digital dimension, with cybercrime definitively overtaking traditional crime in terms of volume of "business".

In modern symbology, the "boy with the hoodie" is replacing the "man with balaclava and gun", without fully communicating the aggressiveness and danger of digital crime. While it is true that within the scope of cybercrime we can also include the small-time hacker, the reality is that large criminal organisations are repositioning themselves in the digital domain and the level of aggressiveness of these organisations is constantly increasing. Without entering into the geopolitical dimensions of cybercrime, the interweaving between criminal organisations and state entities, we can nevertheless be certain that the "boy with the hoodie" no longer accurately represents cybercrime.

To understand the dimensions of the phenomenon and its development, we turn to the large amount of information available on the Web that indicates an exponential growth of information crimes, a growth trend whose end state is difficult to predict.

An authoritative assessment can be found in the reports published in recent years by Clusit, the Italian Association for Information Security, which certifies that this quantum leap in cybercrime is producing year after year damages exceeding 500 billion dollars. According to reports, criminal activities such as scams, extortion, and theft of money and personal data have affected almost a billion people worldwide, causing private individuals alone a loss of more than $180 billion. Impressive numbers, which have increased fivefold in the period 2011-2017. According to these reports, the last few years have also seen "the triumph of Malware, of industrialised attacks carried out on a global scale against multiple targets, and of the definitive descent into the reality of states as threat actors".

In fact, in the analysis of the rapid evolution of cybercrime, a worrying pattern emerges with

> *The Clusit report, like other research on the subject, shows how a "dirty war" is being fought daily in Cyber Space between those who attack and those who defend, a war that, to be won, requires the "call to arms" of not only specialists in computer security, but of all individuals who use digital technologies.*

respect to breaches suffered by public and private organisations: research indicates the trigger for most of these breaches is the so-called "human factor". This analysis considered inappropriate behaviour by any member of the organisation who acted as a "door opener" with respect to the strategies used by the attackers.

The percentages vary from research to research, but all agree that the human factor should be assigned a percentage higher than 80%, highlighting how both the small-time hacker and the large criminal organisations have put individuals and their weaknesses at the centre of their attack strategies.

The human factor in Cyber Security

Despite the large investments made in Cyber Security technologies, the Cyber risk to public and private organisations continues to grow. In order to reverse this trend, it is necessary to invest heavily in the human factor, especially in people's level of awareness. This investment must close the cultural gap generated by rapid digital transformation: all economic and social processes have undergone significant transformations, while human capabilities have not had time to evolve and adapt to the risks associated with the transformations.

The problem not only concerns the older generations who often have difficulty interacting with the latest digital technologies. The younger generations, especially the millennials, have a natural propensity to use digital technologies. But they often do so as "unaware users", because no one has ever bothered to give them the cognitive tools to recognise the risk of becoming victims of unscrupulous organisations that, by violating their privacy, try to manipulate their behaviour and choices.

The Cambridge Analytica scandal, which broke out at the beginning of 2018, made popular an issue that has been known for some years, namely the challenges of keeping control over one's personal data in the social dimension. This issue forms the foundation of the continuous evolution of privacy regulations, including the current European GDPR regulation on the protection of personal data, which revises the very concept of privacy in the light of digital transformation. This situation can only be brought under control if all individuals begin to act in a conscientious manner, taking into account the importance of protecting their personal as well as social spheres.

In order to act conscientiously, it is necessary to acquire the cognitive elements that allow us to develop mature attitudes and adopt proper behaviour concerning the risks of Cyber Space. This is a continuous process that combines knowledge and the fine-tuning of certain characteristics like readiness and reactivity into an overall state of *preparedness*.

Increasing people's awareness requires advanced training processes based on a methodology of ongoing training. If the strategies of attack constantly evolve, on a quantitative and qualitative level, then it is necessary for those who must protect themselves to be at the same level of evolution as Cyber criminals.

Better still, to take a step forward in their capacity to identify threats, even unknown threats. This result can only be achieved by constantly adjusting one's level of knowledge and by always keeping one's attention focused on risk factors.

The role of training

As a consequence of what has been described above, it is clear that within an organisation, whether public or private, it is necessary to ensure that non-specialist personnel, i.e. those who do not have specific skills in the field of Cyber Security, follow a training path that leads them to an increasingly conscientious use of digital technologies, social tools and other resources on the web.

This growth path should allow them to acquire a level of shared knowledge that stimulates defensive human characteristics like attention, readiness and responsiveness.

Awareness of risk leads to a more appropriate response to known dangers, but also to a correct defensive attitude against threats not yet known, an attitude that in the cyber world is absolutely necessary given the rapid evolution of attack techniques.

Awareness is also necessary to avoid an overly defensive attitude that carries an irrational perception of risk, producing behaviour that negatively affects the productivity of the individual and the organisation.

A conscientious profile brings a reduction of risks due to the correct combination of knowledge and experience, while at the same time keeping individuals fully productive and not "stuck" by irrational interpretations of the danger.

Characteristics of the training course

To acquire this conscientious profile, you need a training path that contains:

- a theoretical component that increases aptitude;
- a practical component that positively alters behaviour towards both known and unknown threats.

Considering the particularity of the subject, it will be necessary for this training course to be:

- motivational, stimulating the person to feel involved in the training process;
- low impact, compared to normal work activity;
- accessible, avoiding technological jargon that would alienate non-specialist personnel.

Compared to traditional training plans, a CSA plan has unique requirements deriving from the fact that it impacts the entire company population. It must therefore be characterised by short, self-contained training units that are distributed over time, based on ongoing training methodologies, to produce an effective change in attitude and behaviour regarding cyber risk.

Let's state some further requirements of a CSA training course:

People need to transform themselves from potential "unwitting allies" of criminal activity into aware agents of the Cyber Defence system.

- We have already said that it must be low impact to minimise indirect costs associated with employee productivity;
- it must be flexible to minimise operational impact; a few minutes a week when convenient for the user;
- it must use a simple, common vocabulary, geared towards comprehension and the overall effectiveness of the learning process, and not laden with technological jargon;
- it must be distributed over time, with frequent cross-references to concepts already learned to promote the assimilation and development of new attitudes and behaviours;
- it must be intuitive and enjoyable, with multimedia content;
- it must include forms of gaming and competition, which draw the user in and motivate them to respect training schedules;
- it must include recognition and evaluation of effort and credit for the level of learning achieved;

- it must provide benefits both personally and professionally, considering that conscientious behaviour also produces an increase in the safety of the individual, and therefore to their family sphere.

Methods of delivery

From a training point of view, there are normally two ways of delivering training content:

- classroom training
- training on an e-learning platform.

Both have positive and negative elements, but in the case of CSA, traditional classroom training has high-level limitations. First of all, it is a costly method with a high organisational impact, especially if logistical complications are added (distribution across several sites).

But the real limit of classroom training for CSA is that the time frame is too concentrated, which is known to lead to short-term retention. Classroom training is also difficult to update and adapt, which in the case of CSA is a known requirement.

Absorption of content in classroom training is very intense during the delivery of the course but the effects tend to dissipate over time. In the case of CSA, classroom training is more suited to initial launch and information update activities, which mainly respond to communication objectives rather than to training objectives.

E-learning platforms, by their nature, have low unit costs, are more agile and are easier to adopt. The impact on productivity is certainly lower than that generated by classroom training, as they adapt better to the work rhythms of the different figures and roles taking the course. This leads to solutions that are easier to implement.

E-Learning platforms also have their weaknesses, for example a low level of involvement, entailing the risk of premature abandonment of the programme, or, in cases of compulsory training, a lowering of the level of attention and a decay of the learning processes.

In order to minimise these risks, it is therefore necessary that both the platform and the training content are designed according to the most advanced thinking in corporate training. As far as the platform is concerned, ease of use and the application of the highest standards for user interface are fundamental to the success of the training. The training must be connected to a process of "gamification", because games are the most natural form of learning. The user must be involved in constructive competition, where they perceive a collective mission that goes beyond mere individual learning. The concept of team membership will strengthen individual motivation and stimulate participation.

The content itself should also be designed to stimulate learning and participation and should in no way become an obstacle to the learning process. Moreover, the user must perceive the usefulness of learning and understand how the benefits obtained from their commitment are tangible and have a positive impact on a specific scenario, in this case the interaction with digital technologies.

There is no doubt that CSA requires the adoption of an e-Learning platform, but at the same time it is essential that it is an advanced platform, with content that meets equally advanced training criteria.

Cyber Guru

The Cyber Guru solution gives a concrete response to these awareness-raising issues through the development of a line of Cyber Security products that target the non-specialist staff of public and private organisations.

The main purpose of these products is to contribute to reducing cyber risk by targeting the human factor through advanced training models that develop awareness of threats.

Cyber Guru, with its two solutions, Cyber Guru Awareness and Cyber Guru Phishing, aims to deliver a concrete and effective impact on attitudes and behaviour, transforming people from unwitting vehicles of cybercrime to "active agents" of the Cyber Defence system.

Cyber Guru Awareness

Cyber Guru Awareness is an advanced computer-based training system for Cyber Security Awareness that teaches the fundamental cognitive elements pertaining to Cyber risks and threats.

Cyber Guru Awareness, developed in Italy, is a platform that applies the most modern educational and pedagogical theories, as well as the most current design paradigms, to ensure maximum ease of use by a highly heterogeneous user base.

The training is structured into 3 training levels. Each level is made up of 12 blocks corresponding to a complete and self-contained training cycle.

3 training levels

Levels are structured into 12 training modules, each of which is dedicated to a specific topic, with frequent references between modules. The modules are enabled with a frequency of one per month, and the training path is rigidly sequential. It is therefore necessary to complete one module before moving on to the next.

3 lessons per module

Modules consists of 3 short lessons, each of which is made up of several minutes of video content or, as an alternative, a PDF document that reproduces the same content in rich text format.

The 3 lessons within a module are organised according to this scheme:

- The first lesson provides the basic knowledge. It instils an awareness of the subject, providing the cognitive elements that allow the user to understand the risk.
- The second lesson digs deeper, stimulating "readiness" and conditioning the user to recognise threats even when they present themselves in an unusual and sophisticated form.
- The third lesson provides best practices. It instils in the user an appreciation of correct behaviour, stimulating the proper "reactivity" that allows the user to always react in a conscientious way.

Learning tests

To switch from one lesson to another the user needs to pass a learning test consisting of 4 multiple-choice questions. The lesson is considered passed when the user correctly answers at least 3 questions out of 4. The test can be repeated more than once with the best result applied towards the lesson.

In-depth resources

Those who want to deepen their knowledge of the specific topic covered by the module can access the supplementary reading that complements the obligatory lesson content with optional but related content.

Medals

The module is considered complete with the passing of the third lesson test signifying that all three lessons have been completed. If all 3 tests have been completed with a level of excellence, corresponding to 4 correct answers out of the 4 questions proposed, the participant will be awarded a medal at the end of the module. A medal is also awarded when the level of excellence is obtained by repeating a test several times.

Evaluation test and cups

At the end of 3 training modules, called a training block (or quarter), an evaluation test of 5 multiple-choice questions is given. This evaluation test, unlike the learning tests, is "one shot" and therefore cannot be repeated. In the event that the participant has obtained all the medals relating to the 3 training modules that make up the block, the block evaluation test becomes decisive to win a cup. To win the cup the user must give 5 correct answers out of 5 questions.

Ranking

The training course rewards individual performance with ranking and medals. The individual ranking also serves to enhance the team ranking, which we will discuss later.

The following is the scoring scheme:

- 1 point for each exact answer obtained in the end-of-lesson learning test (passing a lesson therefore results in a minimum score of 3 points and a maximum score of 4 points).
- If a medal is won, the user earns a total of 15 points (12 points earned in the 3 lesson tests and a medal bonus of 3 points),
- 1 point for each correct answer obtained in the end-of-block assessment test (maximum score 5 points).
- A bonus of 10 points is awarded to winner of a cup.

According to this scheme the score of a participant at the end of the annual course can range from a minimum score of 108 points to a maximum score of 240 points.

Team organisation and competition

As mentioned above, Cyber Guru Awareness can be organised into teams by, for example, organisational units. Organisation into teams is the first step in the activation of a virtuous competition, a sort of "Cyber Security" championship.

The training path of each participant, enhanced by the scoring scheme mentioned in the previous paragraph, contributes to a classification of teams taking into account the following considerations:

- The team's score is averaged by the number of its members, so that each team, regardless of its numerical consistency, can compete fairly with the others.
- It is permissible for a person to change teams during the training course (organisational movements). In this case, the user's points will be inherited by the new team.

Certificates

The platform allows each participant to download their certificate of participation, which follows a curriculum model, with an up-to-date certification of the training modules the user has passed. There are three levels of certification coming at the 12th, 24th and 36th modules.

Team leaders and supervisors

In addition to the role of participant, Cyber Guru Awareness allows two other roles:

- The team leader is a participant who coordinates and stimulates their team.
- The supervisor is responsible for the overall training project and has a wide visibility of the progress of the project through a series of statistical reports based on the training's objectives.

Statistics and communication

Cyber Guru Awareness provides a set of statistics that allow users to monitor the effectiveness of their training. These statistics represent a further stimulus to meaningful participation, encouraging the participant's involvement in light of the team and the organisation. Among the various information provided, statistics about medals, for example, will stimulate users to match the achievements of others. Statistics are differentiated according to the role (user, team leader, supervisor).

The platform also provides effective communication tools to stimulate full participation. The news section, for example, highlights important news concerning the evolution of the training course and context related to Cyber Security.

In addition, a series of "Student Care" e-mails are automatically generated detailing the training path of each individual, comparing it to that of their teammates and other teams.

All statistics are provided in full compliance with the Privacy Policy and the protection of personal data. Each participant has their own unique indicators, related to the team and the organisation. Otherwise, participants and team leaders only see aggregated data, by team and by organisation. The only personal statistic that can be seen by all are the medals, which highlight the merits of those who have put a lot of effort into the course.

Cyberpedia

To make it even easier to use the platform there is a large tutorial section that clearly describes each functional unit, employing video animation techniques.

The Cyberpedia also allows users to deepen the understanding of concepts and technical terms that are used during the course. As already mentioned, the course uses an extremely common language that avoids any technological jargon. In some cases, however, it is necessary to use more technical concepts and terms, which are explained in the Cyberpedia. This reference can be used to find technical terminology for concepts that, in the training course, are treated using non-technical language.

Gamification

Learning and evaluation tests, individual and team rankings, team organisation, and cups and medals are all elements that help to stimulate virtuous competition that makes the training path more engaging.

Features

Each element of Cyber Guru Awareness has been designed to maximise the effectiveness of training time, minimise knowledge loss, and effectively eliminate management costs.

- ***COMMON VOCABULARY*** - A vocabulary suitable for everyone that avoids technological jargon
- ***BRIEF LESSONS*** - Organised into short, self-contained lessons and modules within an integrated learning path
- ***MULTIMEDIA CONTENT*** - Video lessons featuring an actor-coach, supported by elements of video animation
- ***INTERACTIVE APPROACH*** - Continuous switching between brief educational content and learning assessment tests
- ***PERVASIVE GAMIFICATION*** - A structure for team competition with ranking and virtual prizes
- ***EFFECTIVE REPORTING*** - A series of reports that define the participation both qualitatively and quantitatively
- ***STUDENT CARE*** - An automated system that stimulates active participation with targeted emails
- ***INDIVIDUAL LEVERAGE*** - The platform leverages the participant's performance results into their individual sphere
- ***CONTINUOUS TRAINING*** - Brief lessons spread over time to maintain a high focus on threats at all times (12 / 24 / 36 months)
- ***USER EXPERIENCE*** - The platform is designed for maximum ease of use and optimal absorption of content

The development process

The quality of Cyber Guru Awareness is ensured by a particularly effective and detail-oriented development and update process. The need to make a generally accessible training course dealing with technical topics that until recently were exclusive to specialists of Cyber Security requires the utmost care in every element of the process and the use of the most advanced methodologies from the pedagogical and educational world.

Delivery platform

Before digging into the process, let's take a look at the delivery platform, which is one of the strengths of Cyber Guru Awareness.

The delivery platform is based on the e-learning tool Moodle, which is entirely web-based and responsive and therefore fully accessible from any device, including mobile devices.

Moodle is the most widespread e-learning framework in the world, especially in academic and educational institutions: more than 1,150 organisations of various types from 81 countries have installed the Moodle platform to manage e-learning activities. In Italy it is used by many businesses and by most educational institutions and universities.

User Interface

Only the most current design paradigms have been adopted in the creation of the platform to ensure maximum ease of use by a highly heterogeneous user base.

The user experience design (validated by user samples) centres on the objective of supporting the user in their training based on a vertical system (module > lesson > verification test) that minimises cognitive effort and ensures an easy approach to the material. Users can easily access additional content offered to them while advancing between modules and lessons and, for continuity and simplicity, can quickly resume the training path after looking at the content.

Although the platform offers an extremely simple use model, users have at their disposal video tutorials that help them understand the platform's functionality.

The platform also benefits from a visual and interactive "language" that, centred on colour codes (traffic lights: green, yellow and red) and on page behaviour, communicates clearly and precisely with the user, establishing a "dialogue" that is gradually reduced and refined as the user progresses through the training course.

To guarantee teaching continuity and coherence, a platform has been developed that can be used comfortably in all devices and whose colours, iconic assets and *artwork* provide a sense of freshness and modernity to the *user interface*, further facilitating the path of understanding and interaction with the content.

The development process

Below is a description of the main phases of the content production process for Cyber Guru Awareness:

- **Content Definition** - this is managed by the Technical and Scientific Committee of Cyber Guru, the specialist entity that selects and processes content. This entity proposes and defines topics and selects the base material. It is made up of experienced Cyber Security specialists with various certifications.
- **Content Transformation** - this is the part of the process in which specialist content is transformed into common language and broken down into the lesson structure (knowledge, in-depth analysis, best practice). This part of the process is led by communication experts who have proven experience in IT and IT Security.
- **Multimedia** - in this phase, managed by experts in multimedia communication, the content undergoes an initial adaptation to the language of video.
- **Training** - in this phase, managed by training experts and conducted with the collaboration of the Department of Science and Education of the University of Rome III, the content is further adapted with respect to the most advanced criteria of the pedagogical and educational sciences, with the aim of making them more effective therefore maximising the involvement of the participants. This is the phase in which questions are created according to the multiple-choice question scheme.
- **Screenplay** - This is the first phase of video production, in which the content takes the form of dialogues and directions for the production phase. This phase is managed with the collaboration of experts in video and multimedia production.
- **Video Production** - this includes all stages of production and post-production, managed by professionals in video and multimedia production. At the end of this process, the content has taken its final form and is ready for the review process.
- **Content review** - at this stage all entities involved verify the quality of the content production process and the effectiveness of the result obtained. Any necessary changes are made and the training form is finally issued.
- **Release** - this is the phase in which the contents are definitively structured into lessons, tests, and in-depth supplementary resources, and inserted into the training module.

The first level of training

Below is the well-thought-out list of the 12 training modules that make up the first level of training. Although each module is self-contained, the sequence in which they are organised has been designed to produce natural references to arguments already addressed previously, thus reinforcing the level of learning and memorization of content.

PHISHING

Phishing is the most common attack technique used by Cyber criminals. The primary method of dissemination is email. However, it can easily be extended to other channels such as messaging and social apps. It is particularly devious because it is based on a convincing deception leading the potential victim to take an action that enables the criminal to launch the main attack. This training module provides the cognitive elements needed to recognise a Phishing attack and to adopt the necessary countermeasures.

PASSWORDS

Passwords are one of the pillars of Cyber Security, the key to IT resources that require guaranteed protection through secure and confidential access. Therefore, password management is one of the basic elements of a defensive strategy for individuals as well as organisations. This training module provides the cognitive elements necessary for the safe management of passwords, protecting them from hacking attempts that may have disastrous consequences.

SOCIAL MEDIA

Social Media represents a new mode of socialisation based on the wide possibilities offered by today's digital technology. But at the same time, it constitutes a risk. Both the privacy of the individual and the security of the organisation's systems can be compromised. This module provides the cognitive elements needed to conscientiously and correctly use these tools, protecting the individual and the organisation from the risks that come with sharing of personal and professional data online.

PRIVACY & GDPR

The introduction of the new European data protection regulations has highlighted the importance of privacy and the protection of sensitive data to organisations. Beyond the specific roles identified by the GDPR, it is important that all members of an organisation have a greater understanding of data protection. This module provides the cognitive elements needed to take a proactive attitude towards data protection and to contribute to the organisation's compliance with the new European standards.

MOBILE & APPS

Mobile devices, especially smartphones and tablets, are becoming increasingly indispensable and highlight the risky overlap between our personal and professional lives. This module provides the cognitive elements needed to safely use mobile devices, both personal and professional, enabling good practices that increase the level of security and data protection.

Mobile & App

FAKE NEWS

Fake News comprises articles containing deliberately fabricated or distorted information, written with the intention of propagating misinformation. They are a dangerous phenomenon, which, if not controlled, can have negative repercussions for both the individual and the organisation. This topic is often viewed from social and political points of view, but it also has a direct connection to Cyber Security. This training module provides the cognitive elements necessary to recognise Fake News, fostering an investigative mentality that helps employees develop the right approach to any information acquired on the internet.

Fake News

USB STORAGE

USB storage, as well as all external memory devices, is critical in the battle to protect confidential information. For this reason they are often subject to specific policies. This training module provides the cognitive elements needed to recognise all of the risks associated with external memory devices, enabling sound practices that avoid data loss and theft.

Memorie USB

EMAIL SECURITY

Email is an increasingly important tool that plays a central and particularly critical role in our professional lives. Sensitive information can easily be shared through email. Therefore, the need for email security should not be underestimated. This training module provides the cognitive elements to safely handle emails and the information they contain.

e-mail Security

MALWARE AND RANSOMWARE

MALWARE in general and RANSOMWARE in particular have quickly come to dominate the headlines, highlighting all their associated risks. Employees must understand that anti-virus software alone does not guarantee total protection against these malicious programs. This training module provides the cognitive elements needed to reduce the risk of falling victim to this particular type of software and to limit the negative consequences in case of an attack.

Malware & Ramsonware

WEB BROWSING

The commonplace activity of browsing the internet exposes us to many risks. A sound knowledge of particular characteristics of websites and browsers can help significantly reduce the organisation's exposure to risk. This training module provides the cognitive elements necessary to understand how to surf the web safely.

CRITICAL SCENARIOS

As we interact with Cyber Space we need to be aware of some critical scenarios: the use of Cloud platforms, business or personal travel, and the use of e-commerce platforms, both B2B and B2C. These use cases are particularly exposed to the possibility of attack by Cyber criminals, with both personal and professional implications. This module provides essential elements of awareness that help prepare for the often-underestimated threats linked to these particular uses of digital technologies.

SOCIAL ENGINEERING

Social engineering is the mother of all Cyber-attack strategies. It focuses on deception and psychological manipulation to pursue fraudulent aims. To make attacks more effective, the core of this strategy is the acquisition of the intended victim's personal information. This module provides elements of awareness on the techniques used by Cyber Criminals, pulling together elements already covered in the previous modules.

The second level of training

Below is the list of the 12 training modules that make up the second level of training. Although each module is self-contained, the sequence in which they are organised has been designed to produce natural references to arguments already addressed previously, thus reinforcing the level of learning and memorization of content.

CLEAN DESK

Paying particular attention to your own workstation by not leaving critical or sensitive information where it can be seen by unauthorised people is a fundamental part of guaranteeing information security and data protection, and respecting privacy regulations. This module provides practical suggestions and reviews concepts such as data protection and privacy, including GDPR.

PERSONAL IDENTIFIABLE INFORMATION

The discussion returns to personal data, data that identifies a specific person, and highlights the risks of not giving personal data the appropriate level of importance. This module reinforces the importance of protecting personal data from a GDPR perspective. It also looks at some dangerous scenarios that can result from not protecting personal data, which threatens the safety of both the user and the organisation. The primary objective is to increase the user's sensitivity to the need to protect this particular type of data.

INFORMATION CLASSIFICATION

Classification of information is a key factor in enforcing information security. However, it is also one of the least understood by users, often seen as unnecessary administration. Classification of information is fundamental for compliance with standards and regulations concerning data protection. As well as explaining the rationale and the motivation that pushes organisations to develop classification processes, this module helps employees understand how important it is to align their behaviour with these goals.

IoT DEVICES

We are increasingly interconnected and this trend shows no signs of slowing. Technological evolution is leading us towards complete interconnection, a paradigm that no longer concerns only people, but also the things we use. Something that a few years ago would have been considered science fiction is now becoming part of daily life. Not only does this impact our professional lives, but it affects our private lives as well. Appliances, cameras, wearable devices, increasingly intelligent cars - these and other "things" are communicating with each another more and more. This scenario is both increasingly fascinating as

well as disturbing. Each interconnected device, if not properly managed, can become a point of potential security vulnerability. This module explains how to relate to this scenario, proposing appropriate behaviour that protects the security level of both the person and the organisation.


Away from the Office

AWAY FROM THE OFFICE

In this module you will reflect on the Cyber risks encountered outside the safe walls of the office, especially when acting in a professional capacity and interacting with the organisation's systems. The analysis focuses on the main points of vulnerability outside the office and how risks can be mitigated through appropriate behaviour resulting from greater awareness.

SPEAR PHISHING

Returning to Phishing by reviewing concepts already discussed, this module offers users who have already gained a basic level of knowledge the opportunity to deepen their understanding and to increase their ability to recognise a Phishing attack. This module focuses on Spear Phishing, a sophisticated technique that targets a specific individual or group of individuals. Emphasis is placed on techniques used to collect sensitive information through fraud and misrepresentation.


Spear Phishing

Smishing & Vishing

SMISHING & VISHING

These are Phishing techniques that target messaging systems such as WhatsApp, Messenger, Telegram, and SMS. This module uses concrete examples to show the user that even messaging systems, once considered intrinsically safe, can now be the source of danger. Above all, it highlights how inappropriate and careless behaviour not only endangers your own security, but can turn you into a vehicle for attacking your entire network.

PHONE SCAMS

There is an increasingly close relationship between telephone scams and Cyber scams. Often the two techniques are integrated into a more complex and sophisticated attack strategy. Telephone fraud is often used to acquire information that becomes the basis for a Cyber attack. This module uses concrete examples to increase awareness of specific risks.


Phone Scam

SNEAKY PHISHING

This module looks at the evolution of phishing attacks, analysing a technique that compromises the two-factor authentication process that was developed specifically to increase the security level of critical systems and applications. Even two-factor authentication contains points of vulnerability directly related to the human factor, relying on the unwitting cooperation of users.

BLUETOOTH AND WIFI

This module focuses on two technical components that keep users connected while on the move. While they are both key contributors to digital transformation and innovation, they contain risks that can be mitigated through informed use.

DATA PROTECTION

We return to data protection, specifically security and privacy and their relationship to various quality and information security standards, in particular GDPR. This module can be considered an annual refresher of Privacy and GDPR material in terms of compulsory training, even if it has new, more in-depth content than found in the first level.

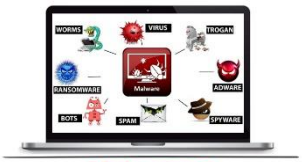
SOCIAL ENGINEERING 2

At the end of each level we return to Social Engineering attack techniques that use deception and psychological manipulation as a basis for achieving fraudulent goals. This module, containing real life examples, goes deeper into the techniques used by Cyber criminals, making it the ideal synthesis of elements already covered in the second level modules.

Real Scam 2

The third level of training

Below is the list of the 12 training modules that make up the third level of training. Although each module is self-contained, the sequence in which they are organised has been designed to produce natural references to arguments already addressed previously, thus reinforcing the level of learning and memorization of content.



Malware 2


Privacy

PRIVACY

In this module, we highlight the value of Privacy and the importance of protecting it. The objective of this module is to provide the cognitive tools needed to recognise that digital technologies, the Web, and Social Media also come with a loss of Privacy. Increased awareness allows us to balance the relationship between Privacy and innovation without paying an excessively high price in terms of confidentiality.


Social & Cyberbullying

SOCIAL MEDIA AND CYBERBULLYING

Let's return to Social Media and the social crisis known as Cyberbullying. As always, our modules address the personal and the professional side of every topic which often have a significant overlap. The content of this module seems to fall strictly in the personal domain and appears to have an exclusively social and cultural impact. However, this is not the case. In addition to providing cultural awareness on this topic, we will show how underestimating this phenomenon may also have security repercussions resulting in legal issues and damage to the image of the organisation.


Legal Aspect

LEGAL ASPECTS

In this module we address the legal aspects related to unintentionally incorrect use of digital technology. Copyright infringement, failure to comply with regulations, unlawful use of software products, defamation - these are just a few examples of potential crimes that could hurt both the individual and the organisation.

REAL-LIFE SCAMS 1

In this module we present case studies of actual scams that have occurred in Cyber space. The primary objective is to raise awareness of how real and immediate danger is. The module will also teach some best practices to help avoid becoming the victim of a scam.


Real Scam 1

REAL-LIFE SCAMS 2

More case studies and best practices. This module provides the tools needed to identify some current scams spreading rapidly due to lack of awareness.

MALWARE 2

A return to the discussion about Malware helps to further understand how careless behaviour can lead to infection of your devices and, as a result, those of your organisation. In this module we provide additional information on Malware, increasing your ability to identify and prevent attacks that are often the first steps in a process that can result in serious damage. During this topic we take into account growth in Cyber awareness made by the user during their training.

e-COMMERCE

This module returns to an area touched on briefly during first level training. This topic is particularly sensitive because risks and potential damage are greater for activities that are directly connected with the flow of money, as in the case with e-Commerce. We take a 360-degree approach as we consider the types of e-Commerce, from B2C to B2B, that have the largest impact on an organisation.

HOLIDAYS AND BUSINESS TRIPS

This module returns to an area touched on briefly during first level training. The theme is holidays and business trips, situations where our cyber vulnerability always increases. We tackle this by considering the entire journey - from planning to returning home or to the office - observing the risks associated with each phase.

CYBER HYGIENE

Maintaining devices in a state of good hygiene helps achieve greater results in terms of productivity, but more importantly it reduces the risks facing information security. We must always maintain a sound device maintenance strategy, including correct care and maintenance of content and all data in general. This module provides a series of best practices on how to maintain the hygiene of our devices and above all the safety of data that can be accessed through them.

BACKUP AND RESTORE

Having the right data recovery strategy allows employees and organisations to protect themselves from the risk of damage caused by a successful Cyber attack. This module creates awareness about what can be a strong defensive asset, one that helps us avoid becoming the object of ransom, as happens in the case of a Ransomware attack, or finding ourselves in the situation where we've lost important data rather than simply having faced a trivial technological event.

BEST PRACTICES

The entire training course focuses on best practices, i.e. good behaviour that helps mitigate Cyber risks. This module emphasises 12 best practices to reducing Cyber risk.

SOCIAL ENGINEERING 3

At the end of each level (a block of 12 modules) we look at Social Engineering attack techniques that use deception and psychological manipulation as a basis for achieving fraudulent goals. This module, inspired by some real-life examples, provides additional elements of awareness about techniques used by Cyber criminals, making it the ideal synthesis of the elements already covered in the third level modules.

Cyber Guru

Cyber Security Awareness

Cyber Guru is a company created by the Daman Group initiative - www.gruppodaman.it - and its international partners with the goal of offering the most advanced training courses on the topic of Cyber Security

www.cyberguru.eu
contact@cyberguru.eu
Phone number +39.06.5159281