CYBER ATTACKS

AWARENESS IS NO LONGER OPTIONAL

CYBER ATTACKS
AWARENESS IS NO LONGER OPTIONAL

EXECUTIVE SUMMARY

The exponential growth of successful cyber attacks against individuals and organisations, the root cause of which can be traced back to human error, has definitively removed any doubt as to the weakest link in any organisation's chain of defence.

THE TREND OF CYBER ATTACKS IS STEADILY AND RAPIDLY INCREASING.

CYBERSECURITY IS A CROSS-CUTTING PROBLEM THAT AFFECTS THE ENTIRE COUNTRY AND AFFECTS INDIVIDUALS AND ORGANISATIONS OF ALL KINDS INDIFFERENTLY

The human factor, rendered even more vulnerable by the pandemic effect, is now the **primary vector** used by **cybercrime** to insinuate itself into organisations, with increasingly sophisticated offensive strategies.
It is precisely the users, whose behaviour is not appropriate to the complexity of the challenge, who unwittingly open the door to the attackers.

The trend was already very clear before the pandemic. If we start from 2020 by analysing the various reports on the state of cybersecurity, both at the Italian and global level, the picture that emerges is that the **growth of cyber attacks** seems **unstoppable** and that among the various attack techniques used, those characterised by the greatest growth mainly rely on the human factor.
A further confirmation that the vast majority of cyber attacks have a human dimension, which can be traced back to an incorrect action on the part of a user.

The arrival of the Coronavirus pandemic on the economic and social scene has only exacerbated this situation, causing the number of attacks to soar. In recent years, the action of cybercriminals has increasingly focused on individuals who, faced with the pandemic phenomenon and its most significant consequences, such as the massive recourse to remote working, have proved to be much more vulnerable than perhaps the organisations could have anticipated.

The **news** is **full** of successful **cyber attacksbuon**, which have affected organisations from all sectors and of all sizes. Prestigious brands and other lesser-known ones have seen their production activities halted and their reputations compromised. Even the old refrain often cited by many SMEs, "a hacker wouldn't be interested in us", has been disproved by the facts.

We are fighting a veritable **cyber war.** An asymmetrical war that sees the **attackers** in a **position** of **unquestionable advantage,** especially since the first line of defence consists of defenceless civilians who, in most cases, do not even realise that they are under attack.

In recent years, **defence capabilities** at the technological level have undoubtedly improved, but the effectiveness of these investments is constantly being thwarted, by virtue of the **weakest link** theory whereby **"the overall strength of a chain is determined by its weakest link"**. QuaWhen the weakest link, as in this case, consists of users interacting with digital technologies and the Internet, it is clear that technological investments alone are no longer sufficient to stop attacks from occurring.

The only way to recreate symmetry between attackers and defenders is to **invest in** the "**first line of defence**", i.e. **digital users**. It is necessary for every organisation to set up **effective** and **innovative** cyber security awareness programmes. The war, however, can only be won if these investments prove their effectiveness in terms of training, with programmes that are able to make a real impact on human behaviour.

In recent years, the investments made in this area, often insufficient, have been driven more by the need to achieve a minimum degree of regulatory compliance than by the need to achieve effective protection against cyber attacks.

On the other hand, all major regulations and frameworks that make explicit reference to cybersecurity (e.g. the GDPR, NIST, NIS Directive, AGID [...]), have highlighted the issue of end-user training but left ample room for interpretation for organisations in determining what is necessary to achieve compliance with these requirements.

So much room that the initiatives implemented were certainly functional with respect to the need to comply with regulations, but totally ineffective with respect to the real objective: **increasing the protection of individuals and organisations** against cyber risk.

CYBER RISK IS ONE OF THE MOST IMPORTANT BUSINESS RISKS THAT ORGANIZATIONS WILL FACE BETWEEN NOW AND THE NEXT FEW YEARS.

CYBER ATTACKS INCREASINGLY EXPLOIT THE HUMAN COMPONENT, THE REAL WEAKEST LINK IN THE CHAIN OF DEFENCE.

For these reasons, it becomes essential to launch effective and **innovative Cyber Security Awareness programmes** that can **impact human behaviour** and **turn users into the** organisations' first line of defence.

THIS IS CYBER GURU'S SPECIFIC MISSION FROM THE OUTSET: TO CREATE A CYBER SECURITY AWARENESS PLATFORM THAT CAN CONCRETELY HELP ITS CUSTOMERS IN THEIR EFFORTS TO STRENGTHEN THE WEAKEST LINK IN THE CYBERSECURITY CHAIN.

THE CYBER GURU PLATFORM WAS CREATED AND CONTINUOUSLY IMPLEMENTED, USING THE MOST ADVANCED TECHNOLOGIES, PRODUCTION PROCESSES AND PEDAGOGICAL METHODOLOGIES TO ENSURE MAXIMUM USER INVOLVEMENT AND THE ACHIEVEMENT OF THE MAIN OBJECTIVE OF A SECURITY AWARENESS PROGRAMME: PROTECTION AGAINST CYBER RISKS.

1. THE SCENARIO

1.1 THE DIGITAL TRANSFORMATION AND ITS TRAPS

SUMMARY

We can say that 2021 structured the social and economic upheaval triggered by the pandemic in the previous year into a situation of chronic alarm on all fronts.

The forced digital transformation that took place in 2020 and was managed in **crisis mode** has become an **established reality** that society has to come to terms with, for better or worse. One of the most obvious consequences was the growth of cyber attacks, which rode the wave of the previous year by continuing to exploit psychological vulnerabilities and also the gulf between the accelerated process of digitisation and users' awareness of cyber threats, which is still by no means bridged.

THESE LAST TWO YEARS THAT WE HAVE EXPERIENCED WILL UNDOUBTEDLY BE REMEMBERED IN THE HISTORY BOOKS AS THE YEARS OF THE **COVID-19 PANDEMIC** AND ALL THE MOMENTOUS TRANSFORMATIONS THAT SOCIETY EXPERIENCED AS A RESULT OF THIS EVENT.

FOREMOST AMONG THESE IS THE **REPOSITIONING** OF **OUR LIVES** ON THE WEB. IF BEFORE COVID ONLY A PART OF IT DEALT WITH THE WEB ON A DAILY BASIS, TODAY IT CAN BE SAID THAT THE WEB RUNS THE LION'S SHARE OF OUR DAYS.

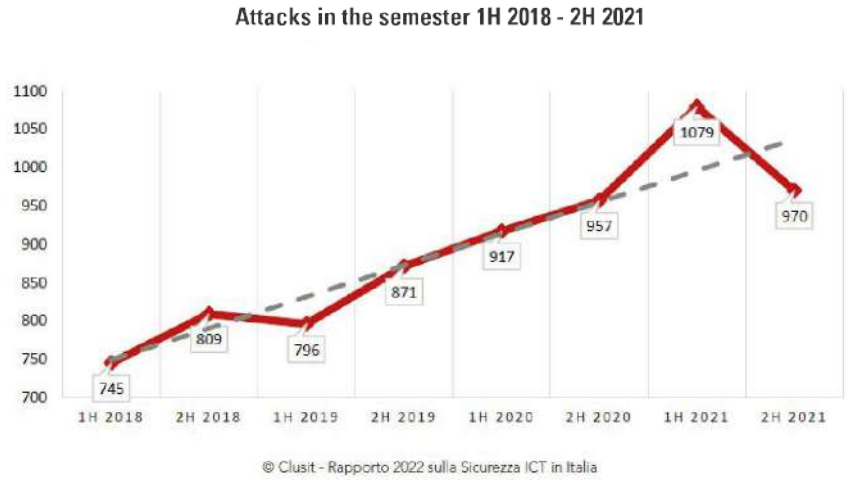
From work, to school, to relationships, to shopping, to information. In short, the web in all its forms can no longer be ignored. This has resulted in a very lucrative opportunity for all those who make **computer fraud** their business, and so **hacker attacks** have become a **widespread and equally dangerous reality**.

So much so that they were described as **"the world's most dangerous weapon"** by **JP Morgan** at its International Council last December, and were identified as "the greatest threat to financial stability, along with climate change" by Christine Lagarde at the annual conference of the European Systemic Risk Board (ESRB). These statements raise a great deal of alarm and are unfortunately confirmed by the data.

According to the **Clusit 2022 Cybersecurity Report**, over the past four years, the monthly average of serious attacks globally has risen from 130 to 171, resulting in a dramatic increase in losses from USD 1 trillion in 2020 to USD 6 trillion in 2021, a 2-digit annual rate of deterioration and 4 times Italy's GDP.

This escalation is mainly due to the **mass use** of **remote working**, which, having started out as a response to a crisis, has become in many situations a new way of working, but also to the increasing adoption of remote learning and online training methods and, last but not least, the use of social collaboration and digital entertainment platforms.

An indisputable sign of this rapid transformation can also be seen in the **growth** of **online shopping**, which, according to data from the Salesforce Shopping Index report, for the first quarter of 2021, saw a **global year-on-year increase of** 58 per cent compared to 17 per cent in the first quarter of 2020.



REMEMBER THAT **ONLINE COMMERCE** INVOLVES PAYMENT METHODS SUCH AS CREDIT CARDS, THE DATA OF WHICH ARE PARTICULARLY ATTRACTIVE TO **CYBERCRIMINALS.** CONFIRMING THE INCREASED DIGITISATION OF SOCIETY, WE CANNOT FAIL TO HIGHLIGHT THE SUBSTANTIAL INCREASE IN BANDWIDTH USAGE. IN THE FIRST MONTHS OF THE PANDEMIC, MANY NETWORK SERVICE PROVIDERS RECORDED SUCH LARGE INCREASES THAT APOCALYPTIC SCENARIOS WERE BEING PREDICTED REGARDING THE RESILIENCE OF THE INTERNET.

Italy led the way, registering a 78% surge that positioned it first in Europe and fourth in the world, after Canada, Holland and the United Kingdom. A **technological quantum leap** that certainly represented and still represents a great opportunity on the road to innovation but which, on the other hand, might result in abrupt if not traumatic crashes.

The point is that all this has happened without a corresponding growth in **digital culture** and therefore without a real ability for users to be able to enjoy digital technologies and the Internet safely. An absence of awareness of threats from the digital world, which has not yet been overcome and therefore continues to provide great opportunities for cybercriminal organisations.

1.2 **CYBER ATTACKS:** PSYCHOLOGICAL AND TECHNOLOGICAL "CRACKS"

SUMMARY

The **unique situation** generated by the **pandemic** is at the origin of the **growth** of **cyber attacks** that started in 2020 and continued to grow stronger in 2021. From this point of view, it is necessary to take into account both the
technological vulnerabilities, linked to remote working, the increase of all online activities and the use of new digital tools such as QR codes, and the **psychological** , vulnerabilities, linked to the **continuous states** of **crisis** and the condition of social distancing. Two important "cracks" into which criminals easily slipped, carrying out attacks that had a disruptive effect on many organisations. The news has been saturated with emblematic cases relating to organisations of all types and all sizes, which have seen their ability to operate cease for longer or shorter periods, with all the consequences, both economic and in terms of image, that such downtime can entail.

THE **PANDCOVID-19 PANDEMIC** HAD A **DISRUPTIVE EFFECT** NOT ONLY ECONOMICALLY AND SOCIALLY, BUT ALSO ON THE **ACCELERATION** OF **CYBER ATTACKS** CLASSIFIED AS **SERIOUS**.

A trend that was already noticeable in 2020 and that saw a sharp increase in 2021. The Clusit report, presented at the beginning of the year, speaks of serious cases on the rise and of Europe being increasingly at the centre of attacks by cybercriminals: a 22 per cent increase compared to 16 per cent in 2020 and 11 per cent in 2019.

The quantitative increase is added to the qualitative one, because the **damage** is much more **serious** for the **affected companies**. Overall, in the four-year period 2018–2021, the number of serious attacks analysed by Clusit increased by 32 per cent, with the government sector (15 per cent) among the most affected categories, followed by ICT and multiple targets.

According to data on **the severity of attacks**, critical level attacks accounted for 32%, high level 47%, medium level 19% and low level only 2%.
Out of the total number of attacks, therefore, the critical and high-level severity attacks hit 80%, whereas the year before, this figure was 56%.

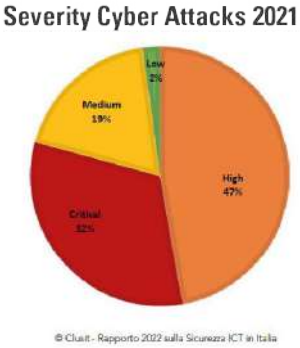
In addition, a recent study produced by IBM security, **Cost of a Data Breach Report** 2021, highlighted how cybersecurity attacks led to the highest costs ever associated with data breaches in the 17-year history of the report, with an average of $4.24 million per incident in the year just ended. In short, if the trend were to continue like this, the outlook would certainly not be rosy.

THE MAIN **DRIVERS** OF THE ACCELERATION OF **CYBER ATTACKS** ARE STILL ANCHORED IN THE TRANSFORMATIONS INSTIGATED BY THE PANDEMIC. ONE OF A **PSYCHOLOGICAL** KIND CONNECTED WITH THE EFFECT ON THE HUMAN PSYCHE OF THE EMERGENCY SITUATION, THE OTHER OF A **TECHNOLOGICAL** KIND ASCRIBABLE TO THE MASSIVE RECOURSE TO FORMS OF TELEWORKING AND THE INCREASED USE OF THE NET FOR EVERYDAY ACTIVITIES.

The **psychological level** has generated states of anxiety and fear typical of crisis situations, with the loss of traditional **reference points**, the obsessive search for news and information and the difficulty of discerning between true and false information, a difficulty that is also emphasised by the advanced fabrication techniques of **fake news**.

Taking advantage of these much more widespread states of anxiety in the population compared to the pre-Covid period, **phishing campaigns** have multiplied, targeting Covid themes in all their guises: the different variants of the virus, the Green Pass, and all the often alarmist information revolving around the pandemic.

The user then found themselves more isolated and more likely to lose their usual points of reference within the company or organisation, which are difficult to retrieve by using social collaboration tools alone.
In addition, in the specific context generated by the pandemic, home spaces have often been and still are shared with other family members operating in the same manner, whether for professional or educational reasons, thus creating critical conditions from the point of view of computer security.



THE SHARING OF DEVICES, OF THE NETWORK, BUT ALSO UNCONSCIOUS ACTION DUE TO PHENOMENA INDUCED BY DISTRACTION, BECOME ELEMENTS THAT PLAY TO THE ADVANTAGE OF CRIME.

Given that the **weakest link** is always **human behaviour**, in a situation of widespread health concern, attention to the right behaviour online has been penalised, throwing the doors wide open to **cybercriminals** who, as refined connoisseurs of the human psyche, **slip right through** the cracks of **emotion**.

Added to this is the **technological level**: remote working is based on a complex architecture that often makes use of the user's private devices, which are less secure by definition and are equipped with hardware configurations.
Again, it is the human factor that is of greatest concern because the gap that exists between the **speed** of the **digital transformation process** and the **speed** at which **people** adapt to this new socio-economic dimension remains, to this day, entirely in favour of cybercrime.

Just think of the **risks that emerged** with the massive increase in the use of **QR Codes**, increasingly used to resolve problems related to pandemic restrictions or to provide more innovative and effective services.

A tool that, like all technology, can greatly facilitate everyday life but that must be "handled" with care because it has the potential to **hide dangerous pitfalls**, such as **malware** or **fraudulent sites**. The fact that the majority of users are poorly informed about the opaque aspects of QR codes, and digital tools in general, easily offers the flank to hackers always looking for new ways to access their favourite crime.

1.3 **WAR:** NOT ONLY AT THE FRONTLINES BUT ALSO IN CYBERSPACE

SUMMARY

To complicate this already dramatic situation, at the beginning of this year, we witnessed the start of the **war** in **Ukraine**, which has opened up **further scenarios** on the **IT security** front. Alongside the traditional war, the one waged with firearms, another **war** is being fought, the **cyber** war, waged with another kind of weapon and which has strong repercussions on a global level. But the effects are not yet quantifiable and will probably not be seen for some months, perhaps years.

According to **CheckPoint's monitoring**, attacks on the government and military sectors since the outbreak of hostilities have already grown on a global basis by 21%. An indisputable sign of how the Russian-Ukrainian conflict is, to all intents and purposes, a global conflict and not just confined to the geographical space of the two leading countries.

In this scenario, no European country can rest easy, given the many **institutional voices** that have recently **sounded the alarm** about the cyber vulnerability of their countries, pointing to cyber warfare as one of the greatest risks that can affect us.

Cases of hacker attacks exploiting the **fears** of the ongoing **war** are becoming more frequent. The first to be targeted by hackers were European manufacturing companies, which fell victim to this war and were targeted by an email phishing campaign with the subject **"Supplier Survey: Effect of supply chain from the Ukraine/Russia conflict"**. In the email, the hackers, in disguise, urged recipients to fill in an attached form, which obviously contained malware, to report possible delays and back-up plans.

A fertile ground that exploits the fears generated by the war and the severe supply impacts. Not to mention the various waves of spam and phishing, in which cybercriminals posing as **humanitarian agencies** or **Ukrainian institutions**, have circulated charity and fundraising campaigns in Europe and the US, with the sole aim of stealing money.

But these few examples that we have mentioned are certainly not exhaustive of a dynamic and constantly shifting situation that could lead to upheavals in the geopolitical, financial, and economic equilibrium scenario, which will certainly have consequences for cybersecurity but whose effects will likely take a few months, perhaps years, to be seen.

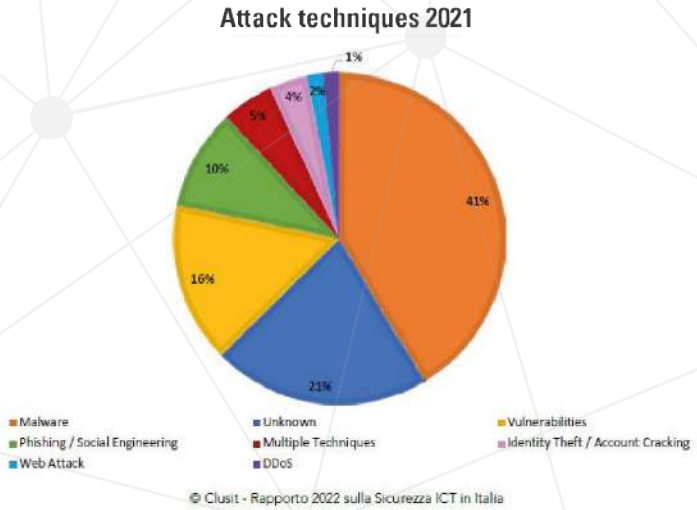
THE **AGENZIA** PER LA **CYBERSICUREZZA NAZIONALE** (THE ITALIAN NATIONAL CYBERSECURITY AUTHORITY) HAS STEPPED UP THE PACE BY WARNING COMPANIES OF THE **URGENCY** OF "... CONDUCTING A RISK ANALYSIS OF THE **CYBERSECURITY SOLUTIONS** USED AND CONSIDERING THE IMPLEMENTATION OF APPROPRIATE DIVERSIFICATION STRATEGIES REGARDING, IN PARTICULAR: ANTIVIRUSES, WEB APPLICATIONS, FIREWALLS, EMAIL PROTECTION, CLOUD SERVICES PROTECTION, AND MANAGED SECURITY SERVICES".

1.4 BEYOND PHISHING AND MALWARE

SUMMARY

While most of the spotlight continues to fall on the phenomena of malware and, of course, phishing, we have already mentioned how all the other forms of attack related to the variety of "cracks", or vulnerabilities, into which criminals manage to slip in order to damage or extort data or money from individuals and companies have exploded over the past year. Among these, the one related to **artificial intelligence and the IoT, the Internet of Things,** undoubtedly occupies a place of honour.

WHEN ANALYSING THE NEW MODES OF ATTACK IN 2021, IT IS CLEAR THAT **CYBERCRIMINALS** ARE BECOMING INCREASINGLY **SOPHISTICATED** AND ABLE TO NETWORK WITH ORGANISED CRIME. AS A RESULT, **THREATS** HAVE BECOME INCREASINGLY **DEVIOUS** AND DIFFICULT TO DETECT AND INCREASINGLY FOCUSED ON EXPLOITING ALL ENTRY POINTS CONSIDERED TO BE THE WEAKEST, INCLUDING INDIVIDUALS.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

The **Clusit 2021 report** shows that more than half of the targets hit were victims of malware and its vulnerabilities. Basically, cybercriminals have mainly relied on the **effectiveness** of **malware**, now produced industrially at increasingly lower costs, and on the exploitation of any weak link that might represent an opportunity for their purposes.

With this in mind, the **rapid development** of **digital technologies** and applications using artificial intelligence, which is undoubtedly an important opportunity for all humanity, cannot go unnoticed. If, a few years ago, we had seen our best friend talking to the refrigerator, we would have thought of calling a doctor or advising him to take a long holiday, whereas today, it already seems like the most normal thing in the world. Yes, because our daily actions are becoming increasingly entangled with artificial intelligence tools that replace humans not only in actions but also in thought. So much so that sometimes it is difficult to understand where one ends and the other begins..

SMART CITIES, SMART BUILDINGS, SMART OFFICES, SMART HOMES, SMART DEVICES, SMART WEARABLES; THE FUTURE OF WESTERN MANKIND SEEMS TO BE IRREVERSIBLY ON THE PATH TO MAXIMISING PERFORMANCE WITH MINIMAL EFFORT.

We are talking about a revolution that affects people both in their individual and in their professional dimension. Indeed, the adoption of IoT systems is also growing in organisations, particularly in real estate automation, and the automotive and healthcare sectors.

It is a **constantly evolving process** that opens the way to an infinite number of possible applications and that, especially when the 5G network becomes widespread, will manage our lives in most of its aspects. This is a fascinating prospect for many, but it also entails great risks.

Without going into the implications that this may have on the functioning of our minds, the **security risk** that is **proportional** to the **use** of the Internet connection must undoubtedly be emphasised. Also because smart devices are often, especially when compared to computers and smartphones, much less evolved in terms of technological defences and could be used as a kind of Trojan horse to infiltrate networks. In short, the perfect prey for cybercriminals.

In fact, in the last five years, IoT-related **cyber attacks have increased by a factor of** 70 precisely because most (around 76%) of the various tools communicate with the network over unencrypted channels, thereby becoming the subject of vulnerabilities that delight hackers.

SUFFICE IT TO SAY THAT THESE ARTIFICIAL INTELLIGENCE SYSTEMS ARE OFTEN INTEGRATED WITH E-COMMERCE SYSTEMS AND CONSEQUENTLY WITH PAYMENT METHODS, SUCH AS CREDIT CARDS OR DIGITAL WALLETS. A TRULY CHERISHED OPPORTUNITY FOR PROFITEERING SCAMMERS.

According to a study conducted by **Kaspersky**, 89% of IoT device owners express concerns about their network security. Among the most common concerns is that of being **spied on by** cybercriminals through **cameras** and **microphones**, or receiving a ransom demand following the blocking of one of the devices, or infecting the entire home network.

These concerns are absolutely justified for both living and working environments, not least because the spread of IoT is seeing irreversible growth.
According to some analysts, by 2025, there are expected to be more than 30 billion IoT connections globally. Given these estimations, potentially each person and each worker will have an average of 4 interconnected devices. Knowledge of the tools required to defend oneself against these risks is therefore of paramount importance

AWARENESS AND THE RIGHT TRAINING ON DIGITAL RISKS REMAIN THE TWO MOST EFFECTIVE WEAPONS.

1.5 **IN THE NEW DIGITAL AGE, SECURITY IS NOT OPTIONAL**

SUMMARY

It has now become evident that life "as it used to be", which many are nostalgic for, may never return and that the impacts of the pandemic will become structural. The confidence we expressed last year about the end of the crisis probably needs to be scaled back. In fact, we have realised that the **crisis** in all its forms is becoming the **new normal** and that we will have to **adapt** as **quickly** as possible to the social and occupational transformations that the health crisis has imposed on us. For this reason, it is necessary to take decisive action on the **human factor**, the true weakest link of the system of defence, with effective Cyber Security Awareness training programmes, a measure now unavoidable to ensure the **security** of **individuals** and **organisations**.

REMOTE WORK IS TAKING ON A **STRUCTURAL DIMENSION**, AS ARE ELECTRONIC COMMERCE, REMOTE LEARNING AND VARIOUS TRAINING PLATFORMS, PUBLIC ADMINISTRATION CITIZEN SERVICES AND UTILITIES COMPANIES.

WHILE **DIGITAL TRANSFORMATION** REPRESENTS A GREAT **OPPORTUNITY** FOR INNOVATION AND **MODERNISATION**, IT INEVITABLY MEANS DEALING WITH AN **INCREASE** IN **SECURITY RISKS**.

Making matters worse is the fact that the new attack methods, as we have seen, are increasingly sophisticated, the social engineering increasingly refined, and often cybercriminals no longer act autonomously but network with their "colleagues" or even with organised crime, producing very damaging effects, especially for companies.

In short, if the future of our lives and business cannot do without digital, this means that **data management**, its **proper use** and **protection** will increasingly be at the heart of any business investment.

A trend that has fortunately been embraced by **Europe** and which has resulted in a commitment to support the **Member States** in their transition to **digitalisation**. In this scenario, it is important to be aware that not all countries in the European Community have the same level of digitalisation, as can be seen from the 2021 edition of the Digital Economy and Society Index (DESI).

In countries with a lower level of digitalisation, it appears that the population between the ages of 16 and 74 have basic digital skills and only 22% have more than basic digital skills.

According to the report, Italy, among the countries in Europe with a low level of digitalisation, "faces significant deficits in basic and advanced digital skills that risk translating into the digital exclusion of a significant part of the population as well as limiting the innovation capacity of businesses".

The choices implemented for the most appropriate placement of the EUR 48.1 billion that the Italian government has decided to allocate to this sector through the **PNRR**, in which **cyber security** occupies a central and strategic place, will therefore be decisive.

Not least because studies published so far on the subject of digital transition indicate that the evolution of data processing and data security will be the trump card for economic recovery. In short, digital innovation, besides being very attractive, is indispensable for the business of the future, but with its development, we also see the growth of its dark side, namely the risk of cyber attacks.

There is only one way to protect yourself: proper corporate training that enables all employees to arrive prepared for the new digitalisation process by avoiding misguided and irreversible clicks.

This requires decisive action on the human factor, the real weak link in the system of defence. Taking action on the human factor and consequently the Cyber Security Awareness training programmes must be considered as a necessary security measure.

Many organisations have **activated** these **programmes** over time with the sole objective of demonstrating compliance with the various regulations that provide, in their standards, for the **training** of **personnel**. In many cases, this has meant a lack of attention to the true effectiveness of **training courses**. But the last two years have shown us unequivocally that this attitude is not helpful, and that in the future, we will have to be more concerned about their effectiveness.

The programmes should be able to concretely transform users' attitudes and behaviour in the face of the cyber threat.

THEREFORE, WHEN CHOOSING A CYBER SECURITY AWARENESS PROGRAMME, ORGANISATIONS WILL HAVE TO TAKE INTO ACCOUNT A NUMBER OF FUNDAMENTAL VARIABLES SUCH AS EFFECTIVENESS, THE TEACHING METHODS USED, THE ENGAGEMENT TECHNIQUES EMPLOYED, THE CONTINUOUS UPDATING ON ATTACK TECHNIQUES, THE ADAPTABILITY OF THE COURSES TO DIFFERENT LEVELS OF AWARENESS, AND, LAST BUT NOT LEAST, THE MULTIMEDIA LANGUAGES USED.

2. TRAINING
2.1 A NECESSARY SECURITY MEASURE

SUMMARY
All organisations that want to take advantage of this now unstoppable digital transformation process must invest in the human factor with advanced and effective training programmes capable of concretely transforming user behaviour, adapting it to the constantly growing and evolving threat level. We are facing an asymmetrical challenge in which the attackers are in an undoubtedly advantageous position. To restore symmetry to this challenge, it is necessary to leverage the human factor which, in cybersecurity, plays a decisive role.

THE DEVELOPMENT OF THE DIGITAL SOCIETY, WITH ITS RISKS, FORCES ALL ORGANISATIONS TO INVEST HEAVILY IN THE HUMAN FACTOR, ESPECIALLY WHEN IT COMES TO RAISING PEOPLE'S LEVEL OF AWARENESS. AN INVESTMENT THAT HAS BECOME NECESSARY TO BRIDGE THE CULTURAL GAP THAT THE EFFECTS OF THE PANDEMIC AND RAPID DIGITAL TRANSFORMATION HAVE EXACERBATED.

The **problem** concerns not only people less familiar with the use of digital technologies, but also the **new generations and millennials**.
The new generations, despite having a natural inclination to use technologies, very often assume a digital posture that can be likened to that of "unaware users", without the ability to recognise the cyber risks behind their actions.

In recent years, we have been accustomed to thinking of **cybersecurity** as a **technological** issue, which concerns only a niche of specialists. The basic idea is that somewhere in our organisation there is always someone in charge of cyber security and that this is more than enough. When faced with a cyber attack, we are inclined to think that the problem is only related to the competence of that team of specialists.

Furthermore, cybersecurity has always been perceived as something that exclusively concerned the professional dimension of our existence. Nothing of direct concern to us. The bias was always the same: **"Why would a hacker be interested in me as an individual?"** In past years, we have experienced this with a certain "lightness": a belief that has affected not only the behaviour of users but also, and this is even more worrying, that of those in management. Today, it is clear that cybersecurity is instead a universal problem that concerns everyone and affects individuals and organisations of all kinds indifferently.

An **asymmetric challenge** that sees the attackers in an undoubtedly advantageous position, not least because the first line of defence consists of "defenceless" people who have no awareness of the threats and the necessary countermeasures. In some cases, users are attacked without even realising it. Following the theory of the weakest link, whereby the overall strength of a chain is determined by its weakest link, we can state that the effectiveness of these investments is nowadays greatly diminished by the weakness of the human factor.

OVER THE YEARS, ORGANISATIONS HAVE BEEN PRIMARILY CONCERNED WITH DEVELOPING DEFENSIVE CAPABILITIES AT A TECHNOLOGICAL LEVEL, AND THESE DEFENCES HAVE UNDOUBTEDLY IMPROVED.

The presence in the field of such a vulnerable element as **users interacting** with **digital technologies** and the Internet gives us a sense of how skewed this battle is in favour of the attackers.

In order to restore symmetry in this challenge, the outcome of which is otherwise already sealed, it is necessary for users to acquire **awareness**, and then, as a consequence, develop attitudes and adapt their behaviour to cyber risks.
A continuous process composed not only of acquiring theoretical knowledge, but also of **training** some human defensive characteristics, such as the **perception** of **danger** and **preparedness**.

While this process should be regarded as a necessary safety measure, it should also be designed and governed according to the typical criteria of training focused on the development of human resources. To increase people's level of awareness, **advanced training programmes** are required, based on innovative methodologies of continuous training, coaching and involvement.
Training platforms that can minimise the impact on those conducting training and cybersecurity management. Only in this way will it be possible to keep pace with the constant evolution of attack strategies, which are becoming increasingly sophisticated, and above all are able to adapt to constantly changing scenarios. We must also consider the need to guide **cognitive learning** in an appropriate manner, without overloading the cognitive system of the learner who, let us not forget, is an extremely busy person and can only devote a few scraps of their attention to training.

IN CYBERSECURITY, THE HUMAN FACTOR PLAYS A DECISIVE ROLE!

2.2 THE ROLE OF TRAINING

SUMMARY

The only way to strengthen the organisations' defensive capacities against **cyber crime** is through a **significant** and ongoing investment in the **"first line of defence"**, that is, **people**. It will therefore be necessary to involve the entire workforce in a **training programme** that allows everyone to make an increasingly conscious use of digital technologies, social tools and resources on the web.
A course of growth that allows them to acquire a level of shared knowledge and that stimulates several human defence mechanisms, such as **attention, preparedness and reactivity.**

Let's try to imagine a fortified medieval city preparing to withstand a siege. Think of a handful of soldiers relentlessly reinforcing the city's perimeter defences, while most of the inhabitants continue to enter and exit the fortifications, leaving the gates open, and among them, some even dig tunnels from the inside out to secure privileged access routes to certain parts of the surrounding countryside.

It seems absurd just to imagine it because the inhabitants of a mediaeval city were perfectly aware of the individual and collective risk that such behaviour would have produced.
Unless they were a conspirator working for the enemy, no citizen would ever even think of weakening their city's defence system with "high-risk" behaviour.

On the other hand, in the **digital world**, behaviours of this type are common, and occur in a climate of total **unawareness**, without a real perception of the **level** of **risk** determined by these behaviours.

FROM THIS PICTURE EMERGES THE CERTAINTY THAT THE ONLY WAY TO RECREATE SYMMETRY IN THE ETERNAL CHALLENGE BETWEEN ATTACKERS AND DEFENDERS IS THROUGH A SIGNIFICANT AND ONGOING INVESTMENT IN THE FIRST LINE OF DEFENCE, NAMELY THE PEOPLE, THE USERS OF DIGITAL TECHNOLOGIES.

We have already pointed out how the human matrix can be found in most attacks, even the apparently more technological ones. The most common triggering vectors can be traced back to behavioural errors on the part of users:

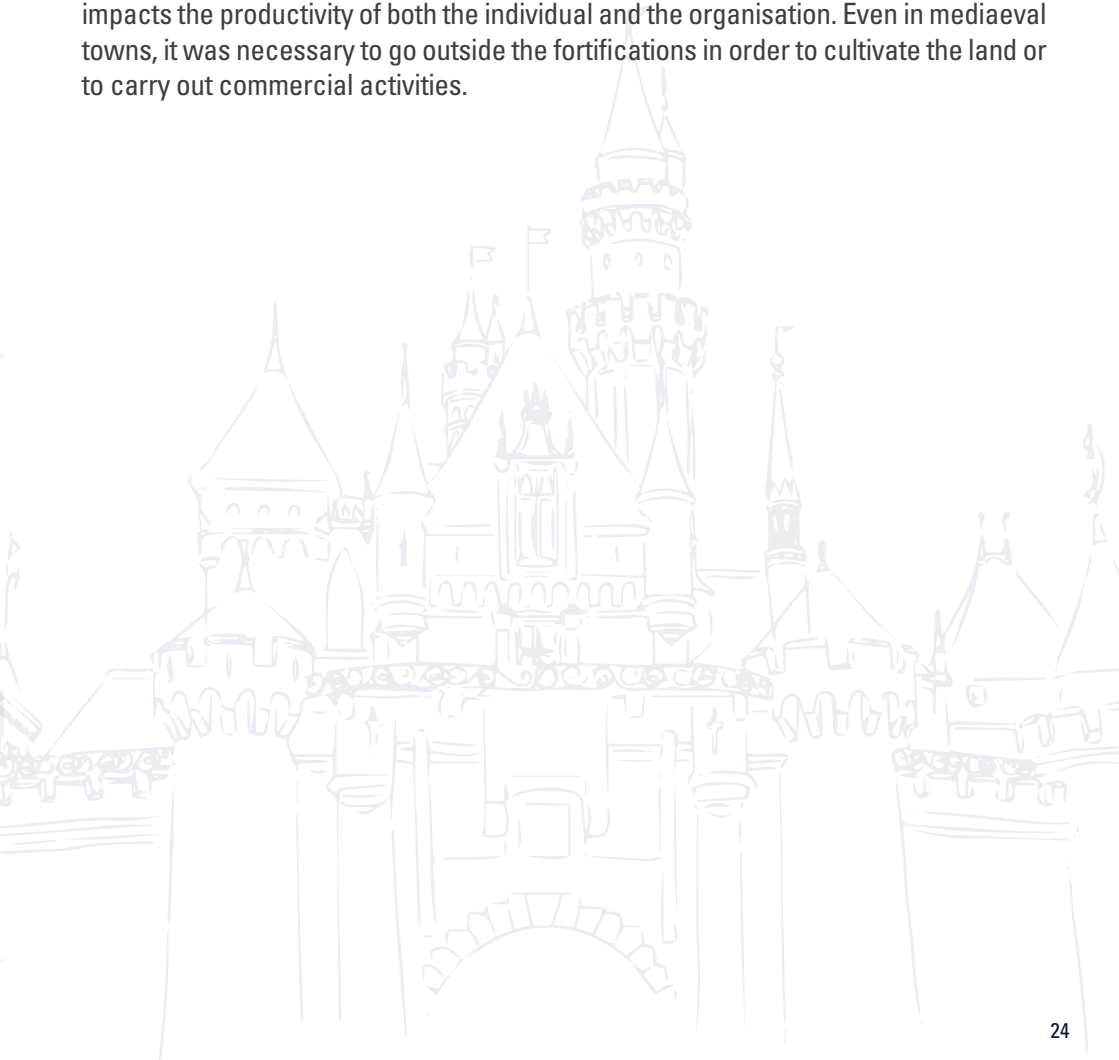
- **THE MANAGEMENT OF DIGITAL DEVICES**
- **INTERACTION WITH MESSAGES, STARTING WITH EMAIL**
- **THE USE OF ACCESS CREDENTIALS AND, IN PARTICULAR, PASSWORDS**
- **LACK OF ATTENTION GIVEN TO THE VALUE OF PRIVACY AND CRITICAL INFORMATION**
- **THE ATTITUDE WITH WHICH PEOPLE SURF THE INTERNET AND APPROACH WEB RESOURCES.**

In order to effectively counter cyber risks, every organisation, public or private, will have to involve the entire workforce, regardless of their role and skills, in a training course that enables everyone to use digital technologies, social tools and resources on the web in an increasingly informed manner.

A **course** of **growth** that allows them to acquire a level of **shared knowledge** and that stimulates several human defence mechanisms, such as **attention, preparedness** and **reactivity**.

Awareness of the **risks** makes us react in a more appropriate way when we are confronted by known dangers, as well as ensuring we have an **appropriate defensive attitude** when facing **potential threats** we don't yet understand, an attitude that is absolutely essential in the cyber world due to the **rapid development** of attack techniques.

Awareness is also necessary in order to avoid an extremely defensive attitude, which, in the face of an irrational perception of risk, produces behaviour that negatively impacts the productivity of both the individual and the organisation. Even in mediaeval towns, it was necessary to go outside the fortifications in order to cultivate the land or to carry out commercial activities.



2.3 **EFFECTIVE METHODOLOGY**

SUMMARY

A training programme that aims to transform individual behaviour must be based on an effective methodology that shows tangible results in terms of learning processes.

A methodology that does not focus exclusively on factual knowledge, but is also able to integrate experiential and inductive paths into the training process. This mix of components will make it possible to develop not only knowledge, but also risk perception and preparedness, creating a generation of aware users, capable of interacting appropriately in the digital sphere, both in their individual and professional dimensions.

A CYBER SECURITY AWARENESS TRAINING PROGRAMME MUST BE BASED ON AN **EFFECTIVE METHODOLOGY**, GEARED TOWARDS AN OUTCOME SUCH AS TRANSFORMING HUMAN BEHAVIOUR, AN **OUTCOME THAT IS PARTICULARLY CHALLENGING TO ACHIEVE.** THE ACHIEVEMENT OF THIS RESULT IS CLOSELY LINKED WITH THE ABILITY TO TAKE EQUALLY EFFECTIVE ACTION WITH REGARD TO LEARNING PROCESSES, BOTH THOSE OF A MORE STRICTLY DIDACTIC NATURE AND THOSE RELATED TO THE UNDERLYING ATTITUDE TOWARDS CYBERSECURITY, BOTH OF WHICH ARE NECESSARY TO PRODUCE A LASTING CHANGE IN BEHAVIOUR.

Training must help to develop the **correct perception** of cyber **risk, realigning** the **rational sphere** with the **emotional** sphere, because today, in most cases, the objective and the subjective dimension are not in balance. On the part of digital users there is in general a **profound underestimation** of the **cyber risk**, or on the contrary, precisely because of the lack of a correct understanding of the phenomenon, attitudes of resistance to the incontrovertible processes of digital transformation can be generated.

An **aware user** is a user who has a clear understanding of network threats and a clear perception of cyber risk, and who has therefore developed an appropriate digital posture. An aware user is also one who is able to understand how the issue of awareness concerns both their private and professional life, and to develop the ability to keep these two dimensions as distinct as possible, because today these two dimensions often tend to overlap.

An **effective methodology** must avoid the mistakes that in previous years have prevented cyber security awareness initiatives from generating the necessary climate of involvement, a primary condition for achieving tangible results on the road to risk reduction. Mistakes that are often inherent in traditional training methods and that in this specific context, since the subject matter is imagined to be particularly difficult, can take on greater significance.

Some of the most widespread **misperceptions** on the subject of cyber security awareness include:

- CYBER SECURITY AWARENESS IS A TECHNICAL DISCIPLINE THAT HAS THE DELUSIONAL AMBITION OF TURNING USERS INTO SPECIALISTS IN THE FIELD OR INTO A KIND OF MODERN SHERLOCK HOLMES CAPABLE OF CARRYING OUT SOPHISTICATED INVESTIGATIONS

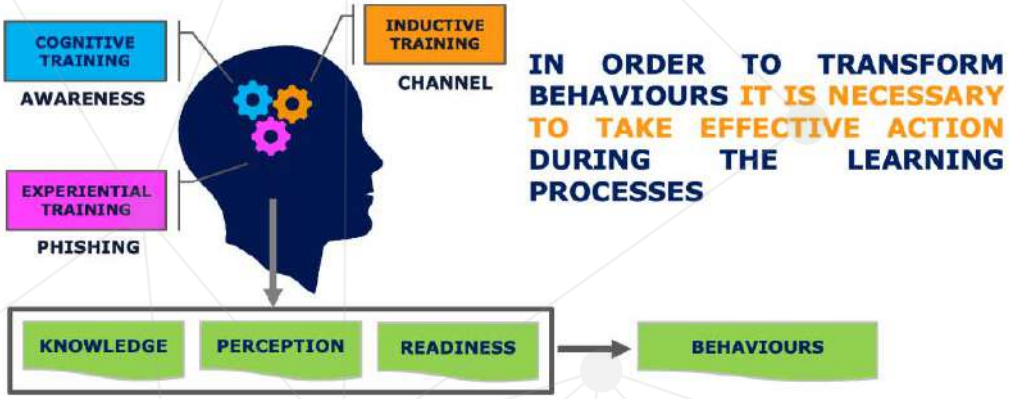
- CYBER SECURITY AWARENESS EXCLUSIVELY CONCERNS THE PROFESSIONAL DIMENSION OF THE INDIVIDUAL AND THEREFORE THEIR ROLE WITHIN THE ORGANISATION

- CYBER SECURITY AWARENESS HAS THE SOLE PURPOSE OF SAFEGUARDING THE ORGANISATION AGAINST AUDIT PROCESSES LINKED TO OBSCURE REGULATIONS AND IS MANDATORY FOR EMPLOYEES

- CYBER SECURITY AWARENESS IS MANDATORY TRAINING THAT DOES NOT PRODUCE USEFUL RESULTS, FOR THE INDIVIDUAL AND FOR THE ORGANISATION

- CYBER SECURITY AWARENESS DEALS WITH THEORETICAL ARGUMENTS THAT HAVE NO PRACTICAL APPLICATION IN THE INDIVIDUAL'S PRIVATE AND PROFESSIONAL LIFE.

Cyber Security Awareness is, in fact, a transversal discipline of an informative nature, which allows people to develop the necessary competence to act securely in the digital sphere, both in their private life, protecting themselves and their social network, and in their professional life, protecting their corporate role and responsibilities, their organisation and the entire ecosystem of which the organisation is part (customers, suppliers, partners [...]).



In order to achieve concrete results, cyber security awareness programmes cannot limit themselves to providing information, but must be structured in experiential and inductive learning paths, following **"learning by doing"** and **"learning by example"** approaches.

By combining didactic training approaches with experiential and inductive approaches, a significant mix is achieved that can positively affect knowledge, perception of danger and preparedness, conditioning attitudes and behaviour.

Although is quite easy to imagine **didactic training**, it is more difficult to picture experiential and inductive training. In the case of experiential learning, the user will have to experience typical attack situations, as in the case of the phishing attack, becoming the target of simulations that reproduce the real experience. In the case of inductive training, this will have to be conducted within real situations, through an effective narrative that produces a process of identification, to the point of users feeling the threat in a more concrete way than they are used to.

2.4 **CONTINUOUS TRAINING**

SUMMARY

Given the specific characteristics and context of the subject matter, a training programme, in order to be effective, must develop according to a model of continuous training, which we could metaphorically define as "homeopathic", and therefore characterised by micro-interventions, diluted over time. This training is not only able to operate at a cognitive level, but also at a perceptual level, therefore enabling the user to develop a real aptitude for recognising the threats of the digital dimension, similar to real-life threats.

IN THE CURRENT HISTORICAL CONTEXT, A CYBER SECURITY AWARENESS PROGRAMME, IN ORDER TO BE EFFECTIVE, MUST DEVELOP IN ACCORDANCE WITH A CONTINUOUS TRAINING MODEL, WHICH REMAINS IN LINE WITH THE DIGITAL TRANSFORMATION PROCESS AND THE EVOLUTION OF CYBER ATTACKS, WHICH PROCEEDS SEAMLESSLY.

In order to sustain a continuous training model, without clearly affecting the productivity of individuals and work teams, it will be essential to proceed with micro-interventions, organised on a regular periodic basis.

The basic principle is that organisations must accustom their workforce to regularly invest a portion of their time (albeit in a manner compatible with their own activities and the need not to overload their cognitive systems) in order to prevent what is already the most important risk to their individual security, and consequently to the security of the entire organisation.

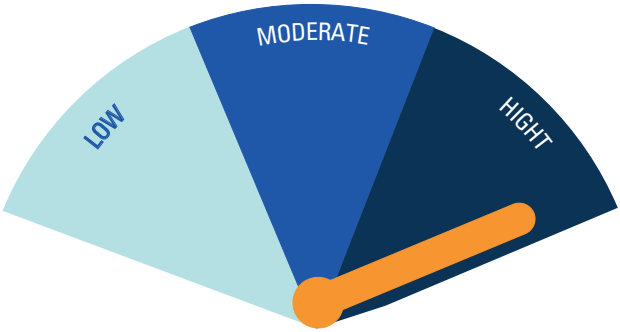
IT IS THEREFORE ESSENTIAL THAT A REAL AWARENESS OF THE RISK LEVEL IS ACQUIRED. BECAUSE CYBER RISK CAN, ON THE ONE HAND, TURN AN INDIVIDUAL'S LIFE INTO A LIVING NIGHTMARE AND, ON THE OTHER HAND, EVEN CALL INTO QUESTION THE VERY SURVIVAL OF THE ORGANISATION.

Cybersecurity today is no longer a technological issue, but a serious business issue, and therefore cyber risk must also be interpreted differently than in years past.

BUT WHAT IS THE RELATIONSHIP BETWEEN CONTINUING TRAINING AND EFFECTIVE TRAINING?

Why should a continuous training model be more effective than one characterised by approaches that are more "concentrated", more intense, and therefore easier to organise, manage and monitor?
Before answering this question, it is necessary to preface it with a preliminary remark: classroom training is not taken into consideration in this analysis, because it is considered less effective in the professional sphere, and because the events that have taken place since 2020 have in fact shown that the only option for dealing with problems of this kind is remote training, in all its various forms.

To return to the two previous questions, it is essential to emphasise again what the real and concrete objective of cyber security awareness training is: to **generate awareness** of **cyber threats** in order to transform the behaviour of all individuals, especially those who have no knowledge or specialisation in the cyber field, which has always been considered a technological field.



AWARENESS LEVEL

In order to transform the behaviour of digital users, enabling them to adapt to the current and future level of threats, it is not enough to work with a didactic model, but it is also necessary to influence perceptions.

The user must develop a real **aptitude for recognising dangers**, developing a fair degree of resilience, so that this sort of instinct can constantly adapt to constantly evolving attack strategies.
At the digital level, we must therefore help users to develop that level of danger perception, which in everyday life saves us from the many threats that surround us.

For these reasons, an **intensive** and **concentrated** training approach can only generate an ephemeral effect, with tangible efficacy only in the immediate future, but which by its very nature inevitably tends to dissipate over time.
Instead, using a "homeopathic" approach, with small interventions diluted over time, allows the perceptive dimension to be maintained at an appropriate level, and also allows the factual dimension to be updated, keeping it in line with developments in the subject. Since cyber threats are constantly changing, taking more and more sophisticated forms, which differentiate them from their original form, it is essential to continue to inject people with small doses of "vaccine" in order to immunise them against these many forms.

BUT WHAT IS AN ACCEPTABLE AMOUNT OF TIME TO DEVOTE TO THIS TYPE OF TRAINING?

WHAT BALANCE SHOULD BE FOUND BETWEEN THE RESULT OBTAINED AND THE IMPACT PRODUCED?

Our experience has shown us how a time commitment of 20 to 30 minutes per month, with a modularity that allows this commitment to be divided into self-consistent training sessions of no more than 10 minutes, is compatible with all kinds of work requirements, eliminating any potential obstructions due to cognitive overload.

Many intensive and concentrated courses, such as the one on safety at work (law 81/2008) or the courses related to the introduction of the GDPR (General Data Protection Regulation), have over the years resulted in unwillingness on the behalf of all employees: a mistake to be avoided at all costs.
In the next section, we will see how a continuous training model, even if it has a low impact on the workforce, must still be supported by techniques to engage the user, who must feel motivated to participate on account of the quality of the content received and the benefits gained.

2.5 **TRAINING INVOLVEMENT**

SUMMARY

An **effective course** must be extremely **engaging** and therefore not perceived as being merely a mandatory imposition. Engagement is highly dependent on languages and formats, but also on the ability to convey the individual benefit that the participant will obtain, a sort of significant cashback with respect to their commitment. This does not mean that such training cannot be classified as mandatory, but any sense of obligation should never be used as a substitute for the use of effective engagement criteria.

A PROGRAMME THAT INTENDS TO BE EFFECTIVE MUST APPEAL TO THE PARTICIPANT, AND DEVELOP IN THEM A SUFFICIENT LEVEL OF ENGAGEMENT. IN ORDER TO ENGAGE THE USER ON A SEEMINGLY DIFFICULT SUBJECT, MISTAKENLY THOUGHT TO BE THE EXCLUSIVE DOMAIN OF SPECIALISTS, IT IS NECESSARY TO OVERCOME THE INSTINCTIVE PREJUDICE OF THOSE WHO, NOT BEING TECHNICIANS, ARE UNABLE TO PERCEIVE THE RATIONALE BEHIND IT.

The first thing to take into account is the language and expressive forms that are used. We are used to conceiving corporate training as something that must be characterised by "heavy" content and forms of expression.

Relying on the canons of traditional training we would run the risk, on a subject whose main focus is cyber threats and the consequences they can generate, of crossing the line into alarmism and technicality, and inducing a situation of denial.

TO ACHIEVE THE OBJECTIVE OF CYBER SECURITY AWARENESS, THE **LANGUAGE USED** MUST THEREFORE BE **HIGHLY INFORMATIVE**, AND **UNDERSTANDABLE** BY EVERYONE. A LANGUAGE THAT CLEARLY EXPLAINS THAT THIS IS NOT A MATTER OF A TECHNICAL NATURE, BUT A **MATTER** THAT **CONCERNS EVERYDAY LIFE** AND EVERY PERSON WHO HAS AN INTERACTION WITH THE DIGITAL SPHERE.

All defensive barriers effect must collapse from the very beginning, giving way to a clear perception of the usefulness of the training initiative and the possibility to fully benefit from it, regardless of one's skill level.

The forms of expression must inevitably be inspired by the principles of multimedia learning and characterised by a high degree of interactivity. The modern and captivating aspect must never be "weighed down" by excessive use of animations, which must be kept in balance with the human element. The coaching function will therefore continue to be interpreted by the human element to foster the identification process based on the teacher/pupil model.

Cyber security awareness is an investment in the human factor, and this connotation must also be reflected in the training programme. Interactivity takes on concrete relevance in the logic of a continuous alternation between short training content and learning tests, which serve to reinforce understanding of the content, following the logic of the university lecture rather than the logic of the final exam. Another form of involvement is related to the benefit derived from training, what we can call "individual leverage".

It is crucial that the participant understands from the very first lesson that the primary benefit of cyber security awareness is for the individual and their social network, even before their organisation. This conviction mitigates the imposing nature of the training itself and the idea that it is only required to protect the organisation from possible consequences.

Only by perceiving this kind of benefit will individuals' involvement be wholehearted, and the incentive to keep their level of awareness of cyber attacks up-to-date will be automatic. This sense of spontaneous involvement will be further enhanced if the identification process is reinforced by continuous reference to real cases and situations, in which it is easy to recognise ourselves.

Often, when embarking on a course of this kind, the question we are most frequently asked by internal managers is whether this training should be classified as compulsory or whether we should mainly focus on involving people. In all honesty, there is no single answer to this question, because each organisation has its own dynamics.

There is no doubt that maximum effectiveness is achieved by combining these two types of levers: that of obligation and that of involvement.

WHILE IT IS TRUE THAT THE COMPULSORY NATURE OF A TRAINING PROGRAMME COULD BE NEGATIVELY PERCEIVED AS BEING AN IMPOSITION, IT IS ALSO TRUE, AND EXPERIENCE CONFIRMS THIS, THAT THE LACK OF A COMPULSORY NATURE COULD BE READ AS SYNONYMOUS WITH "UNIMPORTANT".
THIS IS WHY MAXIMUM EFFECTIVENESS IS ACHIEVED WHEN OBLIGATION AND ENGAGEMENT COEXIST IN A BALANCED WAY.

2.6 **GAMIFICATION**

SUMMARY

Play is perhaps the most powerful of the engagement-generating elements in corporate training. Forms of individual gamification, with the granting of virtual rewards, and group gamification, with the development of virtuous competition between different teams, reinforce learning processes and also positively affect team play.

THE FACT THAT GAMES ARE A TOOL THAT FACILITATES LEARNING PROCESSES HAS BEEN KNOWN FOR A LONG TIME, JUST AS THERE IS EVIDENCE THAT GAMIFICATION TECHNIQUES APPLIED TO CORPORATE TRAINING INCREASE THE EFFECTIVENESS OF THE TRAINING ITSELF, POSITIVELY AFFECTING PARTICIPATION BOTH QUANTITATIVELY AND QUALITATIVELY. THIS IS ALL THE MORE TRUE WHEN IT COMES TO REMOTE LEARNING.

By adding motivational elements, **gamification techniques** strengthen the level of engagement with the training course, which, as we have seen, is a key step in achieving an effective outcome.

Gamification can act on an **individual level**, thanks to virtual reward elements, such as the acquisition of badges, medals, cups, [...], which underline all the important steps of the training path and reward the participant's commitment. Gamification can also act at a **group level**, thereby leveraging the sense of belonging and teamwork.

Belonging to a team, and in this sense activating the mechanism of virtuous competition with other teams, generates high levels of involvement and a greater capacity to develop pervasive internal communication processes.

GAMIFICATION TECHNIQUES, AND CONSEQUENTLY THE ABILITY TO CONVERT THE LEVEL OF PARTICIPATION IN THE TRAINING COURSE INTO A SCORE, HELP BOTH PARTICIPANTS AND SUPERVISORS TO IMMEDIATELY UNDERSTAND THE LEARNING PROGRESS ACHIEVED, AND PROVIDES A CONCRETE BASIS FOR EVALUATING THE RESULTS.

2.7 **COMMITMENT**

SUMMARY

The level of commitment within the organisation and the attention of top management are decisive factors, especially with respect to an initiative that is characterised by its cross-disciplinary nature and the criticality of the subject matter.

IN THE AREA OF CORPORATE TRAINING, EFFECTIVENESS IS ALSO CLEARLY FOSTERED BY THE LEVEL OF COMMITMENT AND INVOLVEMENT OF COMPANY STRUCTURES.
THE ATTENTION OF TOP MANAGEMENT ON SUCH A CROSS-SECTORAL INITIATIVE BECOMES A CRITICAL SUCCESS FACTOR FOR THE INITIATIVE ITSELF.

We have already pointed out that cyber risk is in fact a business risk on a par with others, and it is therefore obvious that reducing the threat of this risk must be a goal of the entire organisation and not exclusive to IT/SEC departments.

The involvement of HR and internal communication structures, with the activation of all communication channels, such as the Intranet, becomes fundamental to the success of the initiative and to its long-term continuation.

EXPERIENCE HAS SHOWN THAT WHEN COMMITMENT IS PUSHED TO THE SO-CALLED C-LEVEL, ALL BARRIERS TO PARTICIPATION AND INVOLVEMENT ARE BROKEN DOWN AND THE EFFECTIVENESS OF TRAINING IS DECISIVELY INCREASED.

3. CYBER GURU
3.1 THE SECURITY PLATFORM

SUMMARY
Cyber Guru is the first line of cyber security awareness solutions designed to increase the security level of individuals and organisations. A platform capable of effectively influencing the human factor thanks to an innovative methodology that improves learning processes.

THE CYBER GURU PLATFORM, DESIGNED IN ITALY, IS BASED ON TRAINING METHODOLOGIES THAT ARE THE RESULT OF MULTIDISCIPLINARY WORK, WHICH HAS ALSO BENEFITED OVER TIME FROM THE COLLABORATION OF THE DEPARTMENT OF EDUCATION SCIENCE OF ROMA TRE UNIVERSITY.

All the solutions of the Cyber Guru platform allow you to achieve two main objectives:

- TO INCREASE INDIVIDUALS' AWARENESS OF THE RISKS INVOLVED IN INTERACTING WITH DIGITAL TECHNOLOGIES AND THE WEB;
- TRANSFORMING THE BEHAVIOUR OF INDIVIDUALS, IN ORDER TO ADAPT THEM TO THE PROTECTION NEEDS OF ORGANISATIONS AND TO THE CHALLENGES IMPOSED BY THE EVOLUTION OF CYBERCRIME.

To achieve these objectives, the design and development of the platforms followed precise methodological lines, which take into account the need to effectively influence learning processes.

THE METHODOLOGY IS DIVIDED INTO 3 LEVELS OF TRAINING:

DIDACTIC TRAINING

EXPERIENTIAL LEARNING

INDUCTIVE TRAINING

IN ADDITION, THE METHODOLOGY AT THE HEART OF CYBER GURU TAKES INTO ACCOUNT TWO OTHER CRUCIAL ASPECTS:

- A process of continuous training, consisting of micro-interventions carried out on a consistent and regular basis
- The involvement of the user in this process, making it clear to them that the primary objective of the process is their protection, as an individual integrated within an increasingly interconnected social context.

ALL THIS SERVES TO DEVELOP, CONTINUOUSLY AND PROGRESSIVELY, THREE CHARACTERISTICS THAT INFLUENCE HUMAN BEHAVIOUR WHEN PEOPLE ARE UNDER THREAT, GENERATING THE ABILITY TO REACT CORRECTLY IN ORDER TO PROTECT THEMSELVES AND THEIR ORGANISATION:

KNOWLEDGE
RATIONAL ACTION

PERCEPTION
INSTINCTUAL ACTION

READINESS
IMMEDIATE ACTION

3.2 CYBER GURU AWARENESS

SUMMARY

Cyber Guru Awareness is an innovative integrated e-learning system that allows the entire organisation to be involved in a training course based on a continuous training methodology and the application of gaming techniques to the entire training course.

Cyber Guru Awareness is designed to engage the entire organisation in an educational and stimulating learning process, which is characterised by its "steady and gradual release" approach and some unique features:

- SELF-CONSISTENT TRAINING MODULES WITH MONTHLY ACTIVATION
- A MINIMUM WEEKLY COMMITMENT, COMPATIBLE WITH ANY JOB ROLE
- VIDEO MICRO-LESSONS IN MULTIMEDIA FORMAT
- THE USE OF PROFESSIONAL ACTORS WITH COACH ROLES
- HIGHLY INFORMATIVE LANGUAGE
- AN INTERACTIVE APPROACH WITH CONTINUOUS ALTERNATION BETWEEN MICRO LESSONS AND TESTS
- MULTIPLE-CHOICE ASSESSMENT TESTS
- GAMIFICATION METHODOLOGY, WITH TEAM ORGANISATION
- A MULTILINGUAL PLATFORM
- ADDITIONAL AND CONSTANTLY UPDATED CONTENT.

The **Cyber Guru Awareness training course** consists of self-consistent **training modules**, each dedicated to a specific topic, with monthly activation, covering a period of 12/24/36 **months**.
Each module in turn consists of 3 **short video lessons** of 5 **minutes each**, each linked to a learning **test** with **multiple-choice questions**.
The video lesson, with the **coach actor**, is the key element of the training course which allows, together with gamification, to actively involve the user in the course.

The gamification mechanisms are structured to create the highest level of involvement of both the individual and the organisation, favouring the activation of internal communication processes, also with a view to **team building**.

GAMIFICATION IS STRUCTURED:

- **IN AN INDIVIDUAL FORM**, WITH THE AWARDING OF VIRTUAL MEDALS AND CUPS THAT REWARD USER PARTICIPATION, ALSO IN TERMS OF QUALITY
- **IN AN AGGREGATE FORM**, WITH A TEAM ORGANISATION THAT MAKES IT POSSIBLE TO GENERATE VIRTUOUS COMPETITION BETWEEN DIFFERENT TEAMS, A PARTICULARLY MOTIVATING MECHANISM THAT LEVERAGES THE LOGIC OF BELONGING.

Cyber Guru Awareness, in order to increase user involvement, without overburdening the training provider, makes available an automatic Student Caring feature, which stimulates participation through well-timed notifications.

3.3 CYBER GURU PHISHING

SUMMARY

Cyber Guru Phishing is an innovative anti-phishing training platform, based on an experiential learning methodology. The goal of Cyber Guru Phishing is to maximise training effectiveness with respect to phishing risk: perception of danger, readiness to react to attack, threat awareness.

CYBER GURU PHISHING IS DESIGNED TO TRAIN THE WORKFORCE TO RESIST PHISHING ATTACKS, THROUGH SIMULATED ATTACK CAMPAIGNS, WHICH ARE CUSTOMISED BASED ON THE BEHAVIOURAL PROFILE OF THE INDIVIDUAL USER, THANKS TO AN AUTOMATIC AND ADAPTIVE PROCESS, GUIDED BY THE USE OF ARTIFICIAL INTELLIGENCE TECHNIQUES.

Thanks to its adaptive approach, Cyber Guru Phishing can be considered a real "personal trainer" in anti-phishing techniques.

The simulation campaigns reproduce the real experience and attack strategies adopted by cybercriminals. The learning algorithms used by the platform are able to select attack templates, based on a criterion of maximum training effectiveness.

With each campaign, the adaptive engine selects new templates based on the user profile, increasing, for example, the difficulty level of attacks for users classified as "strong".

The platform follows the following operating scheme:

1. WITH EACH CAMPAIGN, THE PLATFORM AUTOMATICALLY SELECTS ATTACK TEMPLATES AND MAKES THEM AVAILABLE FOR APPROVAL.

2. THE PLATFORM DISTRIBUTES THE ATTACKS ACCORDING TO A CUSTOMISED SCHEDULE AND WITH A MECHANISM THAT BYPASSES THE WORD-OF-MOUTH PHENOMENON.

3. EACH PERSON WHO SUCCUMBS TO THE DECEPTION IS EXPOSED TO SPECIALISED TRAINING WITH RESPECT TO THE ATTACK SUFFERED, REINFORCING THE EXPERIENTIAL LEARNING METHOD.

4. THE EFFECTS OF EACH CAMPAIGN MAKE IT POSSIBLE TO ENHANCE THE RISK INDICATORS MONITORED BY THE PLATFORM, DETERMINING THE PREPARATION AND DISTRIBUTION OF THE NEXT CAMPAIGN.

5. IN ADDITION TO THE CLASSIFICATION OF USERS INTO "WEAK", "INTERMEDIATE", AND "STRONG", THE PLATFORM ALSO MAKES IT POSSIBLE TO PROMOTE THE "DEFENDER" CATEGORY, I.E. THOSE WHO, IN ADDITION TO NOT FALLING FOR THE DECEPTION, RECOGNISE THE ATTACK AND REPORT IT.

6. ALL INDICATORS FEED INTO THE REAL-TIME REPORTING FUNCTIONALITY, WHICH CAN BE ACCESSED THROUGH AN ADVANCED DASHBOARD.

The reports do not merely display the click-through rate of a campaign, but make available reports and indicators that express a clear map of the risk and the real effectiveness of the route taken.

Experiential learning, implemented through Cyber Guru Phishing, proves to be particularly effective in lowering the phishing risk, steadily increasing the entire organisation's level of resistance to cyber attacks and equally consistently reducing the number of users classified as "weak".

This learning methodology is supported by the platform's features, especially its level of automation, which minimises the impact on cybersecurity teams.

3.4 CYBER GURU CHANNEL

SUMMARY

Cyber Guru Channel is a video training course based on an inductive methodology, created using advanced production techniques, typical of a television series, and with engaging storytelling, designed to immerse the user in real-life situations that reproduce the consequences of a cyber attack generated by misguided human behaviour.

The inductive methodology implemented by Cyber Guru Channel is based on the user's immersion in a real situation and a process of self-identification with the cyber threat, which takes a concrete and therefore possible form.

The user gains awareness not by being given information, but through a narrative, which first targets the perception of danger, and then provides factual knowledge.

The knowledge is "induced" by the narrative itself, and reinforced by the in-depth material made available to the user.

The Cyber Guru Channel's platform videos are made with advanced production techniques and particularly engaging storytelling.

In this particular training course, where the key to understanding is involvement in a story, the user is further supported by the availability, within the platform, of the necessary in-depth material, which provides the theoretical framework to increase their level of awareness of the threat at the centre of the story.

CYBER GURU CHANNEL PROVIDES:

- **MULTIPLE VIDEO FORMATS WITH DIFFERENT STORYTELLING METHODS**
- **IN-DEPTH DOCUMENTATION FOR EACH EPISODE**
- **INTEGRATION WITH THE GAMIFICATION MECHANISM;**

- **STUDENT CARING FUNCTIONS, TO MOTIVATE PARTICIPATION;**

- **REPORTING ON THE LEVEL OF USE.**

The level of engagement generated by Cyber Guru Channel is very high and thereby becomes a driver for other training courses focused on cyber security awareness and for internal communication activities designed to spread the culture of cybersecurity in the organisation.

The training videos, integrated into the Cyber Guru platform, are enriched with all the access control, engagement and monitoring components of the platform.


Cyber
Guru

WWW.CYBERGURU.IT