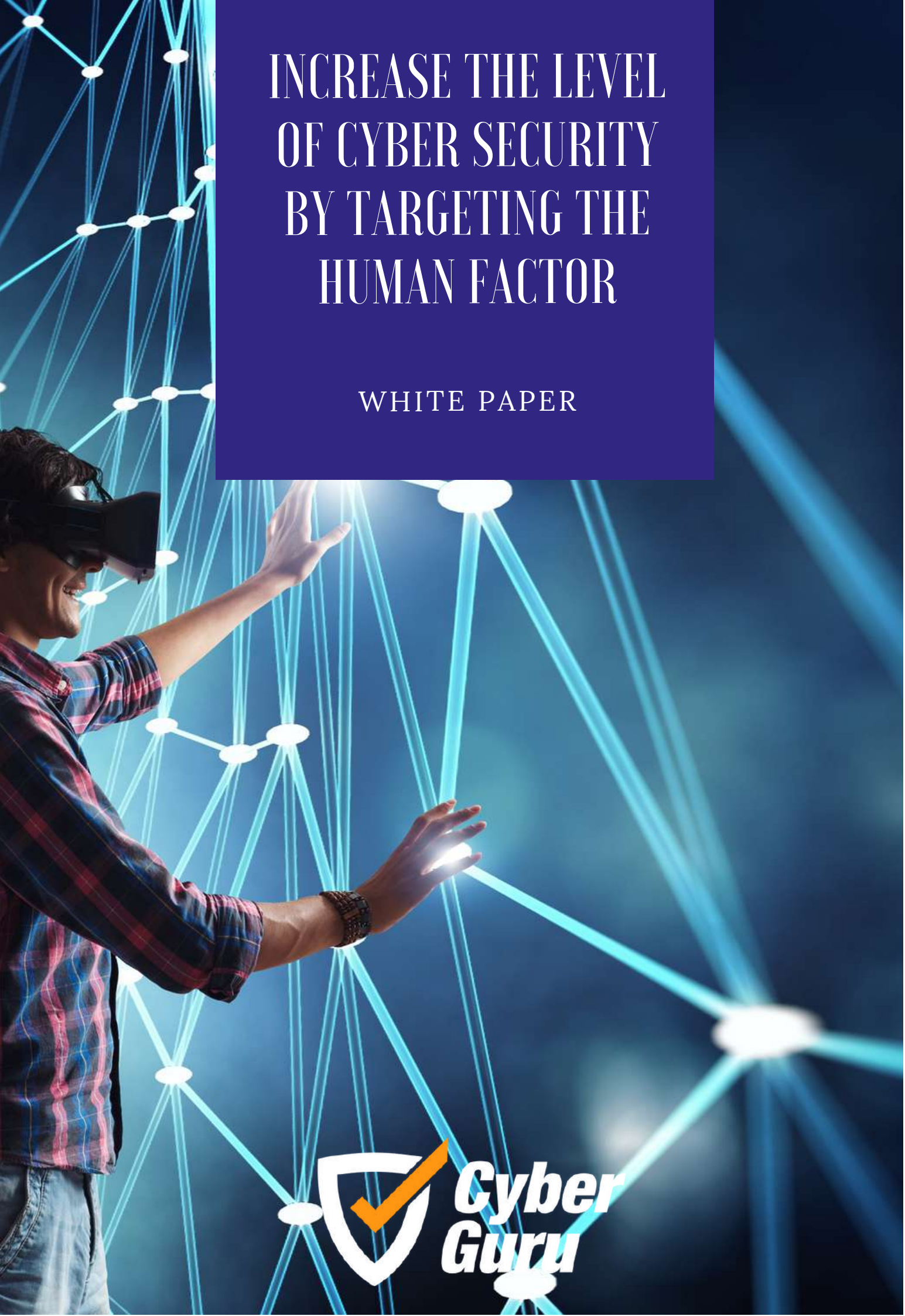
INCREASE THE LEVEL OF CYBER SECURITY BY TARGETING THE HUMAN FACTOR

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.

INVEST ON THE HUMAN FACTOR

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.

REDUCE CYBER RISK

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 GURU AWARENESS

SUMMARY

CYBER SECURITY AWARENESS

INCREASING THE LEVEL OF CYBER SECURITY AWARENESS

Increasing the level of Cyber Security Awareness (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.

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 this case, increasing CSA means **raising the level of Cyber Security for the entire 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**.

DEFINIZIONE

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

Un profilo consapevole è quello che permette di ridurre i rischi usando una giusta combinazione di conoscenza ed esperienza, e che allo stesso tempo mantiene gli individui pienamente produttivi e non “bloccati” di fronte ad un’interpretazione irrazionale del pericolo.

Gli individui devono trasformarsi da potenziali “alleati inconsapevoli” di attività criminali, ad agenti consapevoli del sistema di Cyber Defence.

Security Awareness

IL SALTO QUANTICO DEL CYBER CRIME

Negli ultimi anni si è registrato per molti osservatori il cosiddetto "**salto quantico**" del Cyber Crime, una crescita senza precedenti delle attività criminali che hanno riguardato la dimensione digitale, con il definitivo sorpasso, in termini di volume di "affari", del Cyber Crime nei confronti del crimine tradizionale.
Nella simbologia moderna il "ragazzo con la felpa e il cappuccio" si pone in contrapposizione al "rapinatore con passamontagna e pistola", una simbologia che non aiuta a dimensionare l'aggressività e la pericolosità del crimine digitale. Se è pur vero che all'interno del Cyber Crime possiamo anche considerare il piccolo hacker, la realtà è che **le grandi organizzazioni criminali si stanno riposizionando nella sfera digitale** e che il livello di aggressività di queste organizzazioni aumenta continuamente. Non entriamo nelle considerazioni che riguardano la dimensione geopolitica del Cyber Crime, e quindi degli intrecci che si vanno creando tra le organizzazioni criminali e gli Stati nella gestione del Cyber Spazio, ma è comunque certo che il "ragazzo con la felpa e il cappuccio" è un'icona che ormai non rappresenta più il Cyber Crime.

Per dare una dimensione chiara del fenomeno e del suo sviluppo, possiamo fare ricorso a una grande quantità di ricerche disponibili nel Web, che convergono tutte rispetto a una crescita esponenziale della criminalità informatica, un trend di crescita di cui è difficile prevedere la fine.

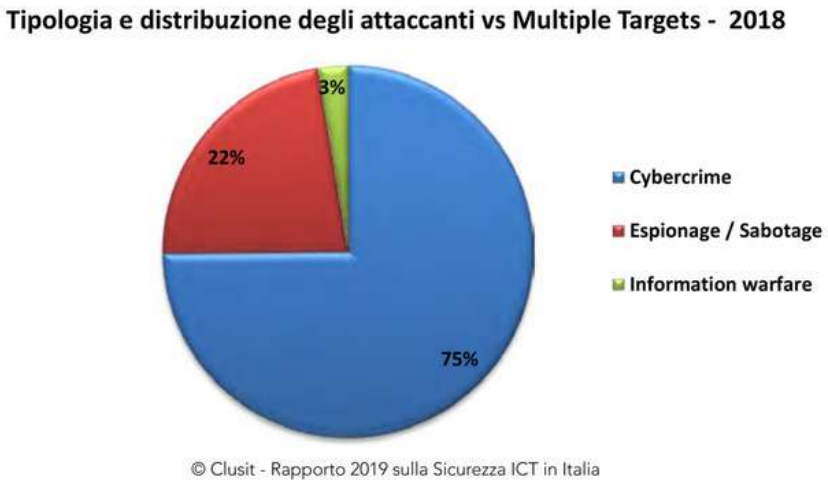
CRESCITA ESPONENZIALE PER LA CRIMINALITÀ INFORMATICA

Una visione autorevole è certamente quella rappresentata dai rapporti degli ultimi anni pubblicati dal **Clusit, l'Associazione Italiana per la Sicurezza Informatica**, che certificano appunto questa sorta di "salto quantico" della criminalità Cyber che, anno dopo anno, sta **producendo danni superiori ai 500 miliardi di dollari**.

Sempre secondo i rapporti, le attività criminali intese come truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita superiore ai 180 miliardi di dollari. Numeri impressionanti, che continuano a crescere anno dopo anno. Dai rapporti emerge che gli ultimi anni continuano a caratterizzarsi per "il trionfo" dei Malware, una delle tecniche più utilizzate dal Cyber Crime".
Un'altra tecnica che continua ad avere una crescita sopra la media è il Phishing e il Social Engineering

Crescita esponenziale

Il rapporto Clusit, come tutte le altre ricerche fatte in materia, mostra come nel Cyber Spazio si consumi quotidianamente una “guerra sporca”, tra chi attacca e chi tenta di difendersi, una guerra che per essere vinta richiede la “chiamata alle armi” non solo degli specialisti della sicurezza informatica, ma di tutti gli individui che agiscono come utenti delle tecnologie digitali.



Infatti, nell’analisi della rapida evoluzione del Cyber Crime, emerge un dato preoccupante rispetto alle violazioni subite dalle organizzazioni pubbliche e private: **tutte le ricerche convergono nel riconoscere come fattore scatenante di gran parte di queste violazioni, il cosiddetto “fattore umano”**. All’interno di questa categoria concettuale, vengono considerati comportamenti inadeguati da parte di un qualsiasi componente dell’organizzazione che di fatto hanno funzionato da “apri porta” rispetto alle strategie utilizzate dagli attaccanti.

Le percentuali variano da ricerca e ricerca, ma tutte concordano sull’assegnare al fattore umano **una percentuale superiore all’80%**, evidenziando come sia il piccolo hacker sia le grandi organizzazioni criminali, abbiano messo gli individui e le loro debolezze al centro delle loro strategie di attacco.

Tipologia di attacchi

IL FATTORE UMANO NELLA CYBER SECURITY

INVESTIRE SUL LIVELLO DI CONSAPEVOLEZZA DELLE PERSONE

A dispetto dei grandi investimenti effettuati in tecnologie di Cyber Security, il rischio Cyber delle organizzazioni pubbliche e private continua crescere. Per invertire questa tendenza è necessario **investire in modo consistente sul fattore umano**, soprattutto sul livello di consapevolezza delle persone. Un investimento che vada a chiudere il gap culturale che è stato generato dalla rapida trasformazione digitale: tutti i processi economici e sociali hanno subito pesanti trasformazioni, mentre le capacità umane non hanno avuto il tempo di evolvere, ma soprattutto di acculturarsi rispetto ai rischi associati a questo tipo di trasformazione.

Il problema non riguarda solo le "vecchie generazioni", che spesso hanno difficoltà anche ad interagire con le tecnologie digitali di ultima generazione, ma riguarda tutti. Le nuove generazioni, in modo particolare i cosiddetti "millennials", hanno infatti una naturale propensione all'uso delle tecnologie digitali, ma lo fanno spesso da "utenti inconsapevoli", perché nessuno si è mai preoccupato di trasferire loro gli strumenti cognitivi per riconoscere il rischio di diventare vittime di organizzazioni senza scrupoli che, violando la loro privacy, cercano di manipolarne i comportamenti e le scelte.

Lo scandalo Cambridge Analytica, scoppiato all'inizio del 2018, ha reso "popolare" un tema che è sul tappeto già da alcuni anni, e cioè la reale possibilità di una persona di mantenere il controllo sui propri dati personali nella dimensione social. Un tema che è stato posto alla base dell'evoluzione continua delle normative sulla privacy, **fino ad approdare all'attuale regolamento europeo GDPR sulla tutela dei dati personali**, che rivede il concetto stesso di privacy alla luce della trasformazione digitale. Un tema che potrà essere posto sotto controllo solo se tutti gli individui cominceranno ad agire in modo consapevole, tenendo conto dell'importanza di tutelare la sfera personale e quella sociale.

Investire sul gap

Per agire in modo consapevole, è necessario acquisire gli elementi cognitivi che consentano di **maturare attitudini e adeguare i comportamenti** rispetto ai rischi del Cyber Spazio. Un processo continuo fatto non solo di conoscenza, ma anche di allenamento di alcune caratteristiche umane, come la prontezza e la reattività, ciò che gli anglosassoni sintetizzano con il termine *readyness*.

Per aumentare la consapevolezza delle persone sono necessari processi formativi avanzati, basati su una metodologia di "**formazione continua**" e di "**allenamento**". Se è vero che le strategie di attacco evolvono costantemente, sul piano quantitativo e su quello qualitativo, allora è necessario, per chi deve proteggersi, di mantenersi allo stesso livello di evoluzione del Cyber Crime, anzi possibilmente porsi un "passo in avanti" rispetto alla capacità di "identificare una minaccia", anche quando questa rientra nel novero delle minacce ancora sconosciute. Questo risultato lo si può ottenere solamente **adeguando costantemente il proprio livello di conoscenza e mantenendo sempre vigile la propria attenzione rispetto ai fattori di rischio**.

IL RUOLO DELLA FORMAZIONE

Come conseguenza di tutto quello che è stato descritto in precedenza, risulta ovvio che all'interno di un'organizzazione, pubblica o privata che sia, è necessario fare in modo che il personale non specialistico, cioè tutti coloro che non hanno competenze specifiche in ambito Cyber Security, seguano un percorso formativo che li porti a fare un uso sempre più consapevole delle tecnologie digitali, degli strumenti social e delle risorse presenti nel web.

Un percorso di crescita che consenta di acquisire un livello di conoscenza condivisa e che stimoli alcune caratteristiche difensive umane come l'attenzione, la prontezza e la reattività. La consapevolezza del rischio porta a **reagire in modo più appropriato** di fronte ai pericoli conosciuti, ma anche ad avere un corretto atteggiamento difensivo di fronte a potenziali minacce non ancora conosciute, un atteggiamento che nel mondo Cyber è assolutamente necessario per la rapida evoluzione delle tecniche di attacco.

La consapevolezza è necessaria anche per evitare un atteggiamento estremamente difensivo, che, di fronte ad un'irrazionale percezione del rischio, produca comportamenti che incidano negativamente sulla produttività dell'individuo e dell'organizzazione.

Prontezza e reattività

CARATTERISTICHE DEL PERCORSO FORMATIVO

Per acquisire questo profilo consapevole è necessario un percorso formativo che contenga:

- una parte più orientata alla nozione, che produce il **miglioramento della componente attitudinaria**;
- una parte più orientata alla pratica, che produce il **miglioramento del profilo comportamentale** verso minacce più o meno conosciute.

Considerando la specificità della materia sarà necessario che questo percorso formativo sia:

- **motivante**, stimolando la persona a sentirsi coinvolta nel percorso formativo;
- **a basso impatto**, rispetto alla normale attività lavorativa;
- **divulgativo**, rifuggendo ogni forma di ortodossia tecnologica che provocherebbe un naturale rifiuto da parte del personale non specialistico.

Rispetto ai tradizionali piani di training, un piano di CSA ha delle caratteristiche di unicità derivanti dal fatto che impatta sull'intera popolazione aziendale.

Dovrà quindi essere caratterizzato da **unità formative brevi, auto-consistenti e ben distribuite nel tempo**, prendendo spunto da metodologie di "on-going training", così da produrre **un effettivo cambio di atteggiamento e di comportamento** di fronte al rischio Cyber.

Percorso formativo

Facciamo alcune ulteriori considerazioni relativamente a un percorso formativo di CSA:

- abbiamo già detto che deve avere un **basso impatto**, al fine di contenere i costi indiretti, legati alla produttività dei dipendenti;
- per le stesse ragioni deve essere **flessibile nella sua fruizione**, al fine di limitare l'impatto operativo; pochi minuti a settimana da poter fare nei momenti ritenuti più opportuni;
- deve utilizzare un **lessico semplice**, divulgativo, finalizzato alla comprensione e quindi all'efficacia del processo di apprendimento, e non al rispetto di canoni di carattere tecnologico;
- deve essere **distribuito nel tempo**, con frequenti richiami di concetti già esposti, per favorire l'assimilazione e lo sviluppo delle attitudini e dei comportamenti;
- deve essere **intuitivo e gradevole da fruire**, con contenuti di carattere multimediale;
- deve includere **forme di gioco e di competizione**, che lo rendano coinvolgente anche rispetto al fattore tempo;
- deve includere **forme di riconoscimento e valutazione** dell'impegno profuso e del livello di apprendimento raggiunto;
- deve fornire **benefici sia sul piano personale che sul piano professionale**, considerando che un comportamento consapevole produce anche un incremento della sicurezza della persona, estensibile alla sua sfera familiare.

Unicità formativa

MODALITÀ DI EROGAZIONE

Dal punto di vista formativo si contrappongono normalmente due modalità di erogazione della formazione. Entrambe presentano elementi di valutazione positivi e negativi, ma nel caso della CSA la tradizionale formazione d'aula presenta dei limiti macroscopici:

LA FORMAZIONE D'AULA

Per prima cosa si tratta di una **formazione molto "dispendiosa" e con un impatto organizzativo elevato**, specialmente se si sommano complicazioni di carattere logistico (distribuzione su più sedi).

Ma il vero limite della formazione d'aula rispetto ai programmi di CSA è dato dalle caratteristiche proprie di questo tipo di intervento formativo, **molto concentrato nel tempo** e che produce risultati effimeri, poco duraturi e che non lasciano molto spazio all'aggiornamento, che nel caso della CSA è invece una vera e propria necessità.

Il coinvolgimento è molto forte durante l'erogazione del corso e tende invece a dissiparsi con il passare del tempo.
Nel caso della CSA, la formazione d'aula si presta più ad attività iniziali di lancio e di informazione, che rispondono soprattutto ad obiettivi di comunicazione, piuttosto che ad obiettivi di carattere formativo.

LA FORMAZIONE E-LEARNING

Le piattaforme di e-Learning, per loro natura hanno costi unitari contenuti, sono più agili e più facili da adottare.

L'impatto sulla produttività è certamente più basso di quello generato dalla formazione d'aula e si adattano meglio ai ritmi produttivi delle diverse figure e dei diversi ruoli. Per questo sono soluzioni di più facile adozione.

Anche le piattaforme di e-Learning hanno i loro punti di debolezza che consistono in un basso livello di coinvolgimento, che comporta il rischio di un abbandono prematuro del programma, oppure, nei casi di formazione obbligatoria, ad un abbassamento del livello di attenzione, con un decadimento dei processi di apprendimento.

Al fine di minimizzare questi rischi è quindi necessario che, sia la piattaforma, sia i contenuti formativi erogati, siano progettati secondo **i dettami più avanzati della formazione aziendale**.

Modalità di erogazione

UNA PIATTAFORMA AVANZATA DI E-LEARNING

Per progettare una piattaforma che segua i dettami più avanzati della formazione aziendale significa sarà fondamentale la sua semplicità di fruizione e i criteri di interfaccia che devono essere realizzati secondo i più elevati standard di User Interface.

La fruizione deve essere collegata a un processo di "**gamification**", perché il gioco è la forma più naturale di apprendimento. L'utente deve essere poi coinvolto in una competizione virtuosa, dove percepisca una missione collettiva che va oltre il mero apprendimento. Il concetto di appartenenza a un team serve a rafforzare le motivazioni individuali e a stimolare la partecipazione.

Anche i contenuti devono essere progettati per **stimolare l'apprendimento e la partecipazione** e non devono diventare un ostacolo al percorso formativo. Inoltre, l'utente deve percepire l'utilità dell'apprendimento e comprendere come i benefici ottenuti a fronte del suo impegno siano concreti, in grado di incidere sulla qualità della sua esperienza, in questo caso l'esperienza nell'interazione con le tecnologie digitali.

Non ci sono dubbi che la CSA per la sue peculiarità richieda l'adozione di una piattaforma di e-Learning, ma nello stesso tempo è indispensabile che sia una piattaforma avanzata, con contenuti che rispondono a criteri formativi altrettanto avanzati.

Piattaforma avanzata

CYBER GURU

LA LINEA DI SOLUZIONI PER LA CYBER SECURITY

Cyber Guru ha lo scopo di dare una risposta concreta a queste istanze di crescita del livello di consapevolezza, attraverso lo sviluppo di un'intera linea di prodotti di Cyber Security che hanno come target il **personale non-specialistico delle organizzazioni pubbliche e private**.

La finalità principale di queste soluzioni è quella di contribuire a **ridurre il rischio Cyber, andando ad agire sul fattore umano** attraverso modelli avanzati di formazione che siano in grado di sviluppare consapevolezza rispetto alle minacce.

Cyber Guru, con le due soluzione **Cyber Guru Awareness e Cyber Guru Phishing**, punta quindi ad **incidere in modo concreto ed efficace su attitudini e comportamenti**, trasformando le persone da veicoli inconsapevoli del Cyber Crime, ad "agenti attivi" del sistema di Cyber Defence.

Soluzioni Cyber Guru

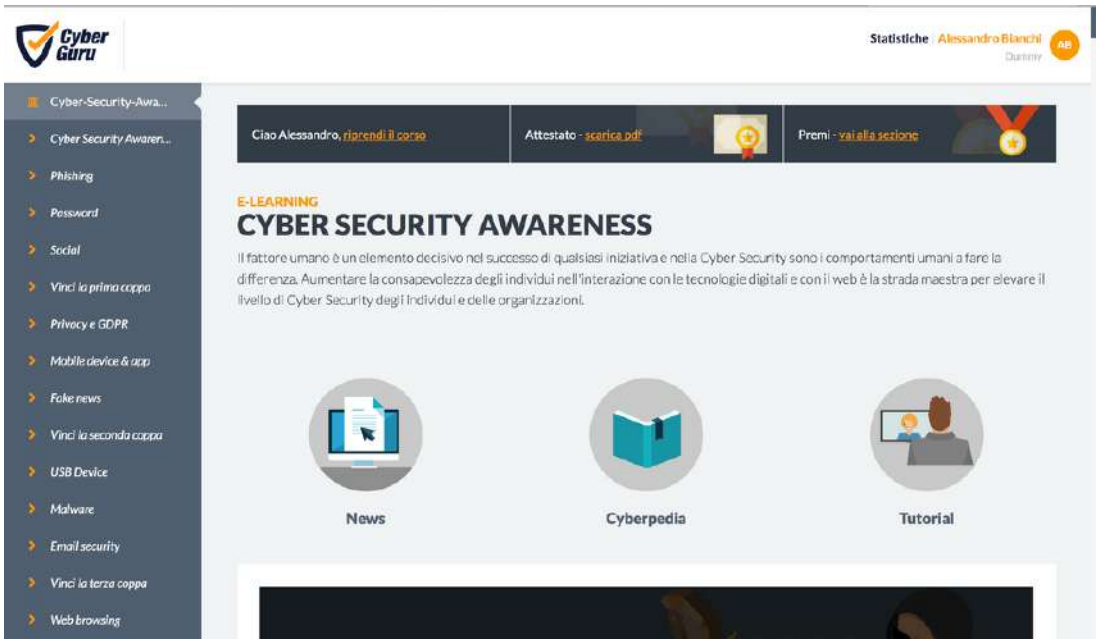
CYBER GURU AWARENESS

IL SISTEMA AVANZATO DI CYBER SECURITY AWARENESS

Cyber Guru Awareness, un sistema avanzato di **Cyber Security Awareness Computer based training**, proposto in modalità e-Learning, che fornisce gli elementi cognitivi fondamentali rispetto ai rischi e alle minacce Cyber all'interno di un percorso formativo che favorisce i processi di apprendimento.

Cyber Guru Awareness è una piattaforma sviluppata completamente in Italia, applicando le più moderne **teorie educative e pedagogiche**, nonché i più attuali e consolidati paradigmi di progettazione orientati a garantire la **massima facilità di utilizzo** da parte di un parco utenti estremamente eterogeneo.

La formazione è strutturata in **3 livelli formativi**. Ogni livello è formato da 12 blocchi corrispondenti a un ciclo formativo completo e auto-consistente.

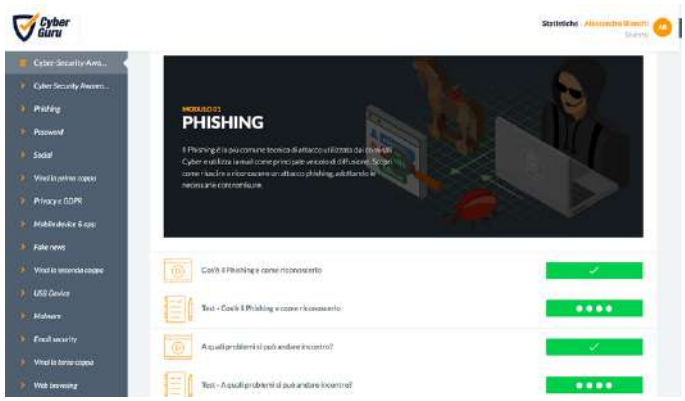


Cyber Guru Awareness

3 LIVELLI FORMATIVI

Ogni livello è strutturato in **12 moduli formativi**, ognuno dei quali è dedicato ad uno specifico argomento, anche se sono frequenti i richiami tra un modulo e un altro.

I moduli vengono abilitati con la frequenza di uno al mese, e il metodo di fruizione è rigidamente sequenziale. E' quindi necessario completare la fruizione di un modulo, prima di passare al modulo successivo.



3 LEZIONI PER MODULO

Ogni modulo è formato da **3 brevi lezioni**, ognuna delle quali è costituita da un contenuto video di pochi minuti e, come alternativa, da un documento pdf che riproduce gli stessi contenuti del video in un formato "rich text".
Le 3 lezioni all'interno di un modulo sono organizzate secondo questo schema:

- La prima lezione è quella della conoscenza di base; consente una presa di conoscenza dell'argomento, fornendo gli elementi cognitivi che consentono la comprensione del rischio.
- La seconda lezione è quella dell'approfondimento; consente di stimolare la "prontezza", creando le condizioni per riconoscere le minacce anche quando queste si presentano in forma insolita e sofisticata.
- La terza lezione è quella delle best practice; consente di acquisire "buone pratiche" di comportamento, stimolando la "reattività", e quindi la capacità di agire in modo consapevole.

TEST DI APPRENDIMENTO

Per passare da una lezione all'altra è necessario superare un test di apprendimento, costituito da 4 domande a risposta multipla. La lezione è considerata superata quando si risponde correttamente ad almeno 3 domande su 4. Il test può essere ripetuto più di una volta e ai fini del percorso formativo viene sempre considerato il risultato migliore.

Livelli e moduli

DOCUMENTO DI APPROFONDIMENTO

Coloro che vogliono approfondire la specifica tematica trattata nel modulo, possono accedere al documento di approfondimento, che integra i contenuti “obbligatori” delle lezioni, con contenuti la cui fruizione è facoltativa rispetto al percorso formativo.

MEDAGLIE

Il completamento del modulo si ottiene automaticamente con il superamento del terzo test di apprendimento, e quindi con l’attestazione del superamento della terza lezione. Qualora tutti e 3 i test di apprendimento siano stati completati con un livello di eccellenza, corrispondente a 4 risposte esatte sulle 4 domande proposte, a fine modulo al partecipante viene assegnata una medaglia. La medaglia viene assegnata anche quando il livello di eccellenza viene ottenuto ripetendo un test più volte.

TEST DI VALUTAZIONE E COPPE

Alla fine di 3 moduli formativi, e quindi di quello che viene definito un blocco formativo (o trimestre), viene proposto un test di valutazione di 5 domande a risposta multipla. I test di valutazione, a differenza di quelli di apprendimento, sono “one shoot” e quindi non possono essere ripetuti. Nel caso di un percorso eccellente, e quindi nel caso in cui il partecipante abbia ottenuto tutte le medaglie relative ai 3 moduli formativi che costituiscono il blocco, il test di valutazione diventa decisivo per conquistare una coppa. Per conquistare la coppa è necessario fornire 5 risposte esatte su 5 domande.

ATTESTATO

La piattaforma consente ad ogni partecipante di scaricare il proprio attestato di partecipazione, che segue un modello curriculare, per cui certifica in ogni momento i moduli formativi superati e definisce tre livelli di consolidamento al raggiungimento del 12’, 24’ e 36’ modulo.

Medaglie e coppe

CLASSIFICA

Il percorso formativo permette di valorizzare una classifica individuale e un “medagliere”. La classifica individuale serve a valorizzare la classifica per team, che tratteremo più avanti.

Di seguito lo schema di punteggio applicato:

- 1 punto per ogni risposta esatta ottenuta nel test di apprendimento, a fine lezione (il superamento di una lezione comporta quindi il punteggio minimo di 3 punti e il punteggio massimo di 4 punti).
- La conquista di una medaglia comporta l'assegnazione di 15 punti (12 punti conquistati nelle risposte ai test delle 3 lezioni e un bonus di 3 punti).
- 1 punto per ogni risposta esatta ottenuta nel test di valutazione a fine blocco (massimo punteggio 5 punti).
- In caso di conquista della Coppa viene concesso un bonus di ulteriori 10 punti.

Per effetto di questo schema un partecipante che arriva a fine corso può produrre da un punteggio minimo di 108 punti a un punteggio massimo di 240 punti.

ORGANIZZAZIONE E COMPETIZIONE PER TEAM

Come già accennato in precedenza, Cyber Guru Awareness prevede un’organizzazione per team, e quindi per unità organizzative. L’organizzazione per team è propedeutica all’attivazione di una competizione virtuosa tra i vari team, una sorta di campionato della “Cyber Security”.

Il percorso formativo di ogni partecipante, valorizzato attraverso lo schema di punteggio citato nel paragrafo precedente, contribuisce in forma aggregata a costituire una classifica dei team tenendo conto delle seguenti considerazioni:

- Il punteggio del team è mediato rispetto al numero dei suoi componenti, così che ogni team, indipendentemente dalla propria consistenza numerica, può competere con gli altri.

- Se una persona cambia team durante il percorso formativo (spostamenti organizzativi) le sue prestazioni verranno ereditate dal nuovo team di appartenenza.

Competizione per team

TEAM LEADER E SUPERVISORE

Oltre alla figura del partecipante, Cyber Guru Awareness, prevede altre due figure:

- Il team leader, che è un partecipante che ha funzioni di coordinamento e di stimolo nei confronti del proprio team.

- Il supervisore, che è il responsabile del progetto formativo e che ha un'ampia visibilità rispetto all'andamento del progetto attraverso una serie di report statistici dedicati alla sua funzione e ai suoi obiettivi.

STATISTICHE E COMUNICAZIONE

Cyber Guru Awareness fornisce una serie di statistiche che consentono di mantenere un monitoraggio completo sull'efficacia del percorso formativo. Queste statistiche rappresentano un ulteriore stimolo ad una piena partecipazione, favorendo il coinvolgimento del partecipante, rispetto al team e all'organizzazione. Tra le varie informazioni fornite:

- il medagliere è uno strumento che stimola l'emulazione positiva. Le statistiche sono diversificate a seconda del ruolo (utente, team leader e supervisore);
- la sezione news consente ad esempio di evidenziare novità importanti che riguardano sia l'evoluzione del percorso formativo sia l'evoluzione del contesto relativo alla Cyber Security;
- le mail di "Student Caring", che consentono di evidenziare il percorso formativo del singolo individuo, paragonandolo a quello del proprio team e degli altri team in competizione.

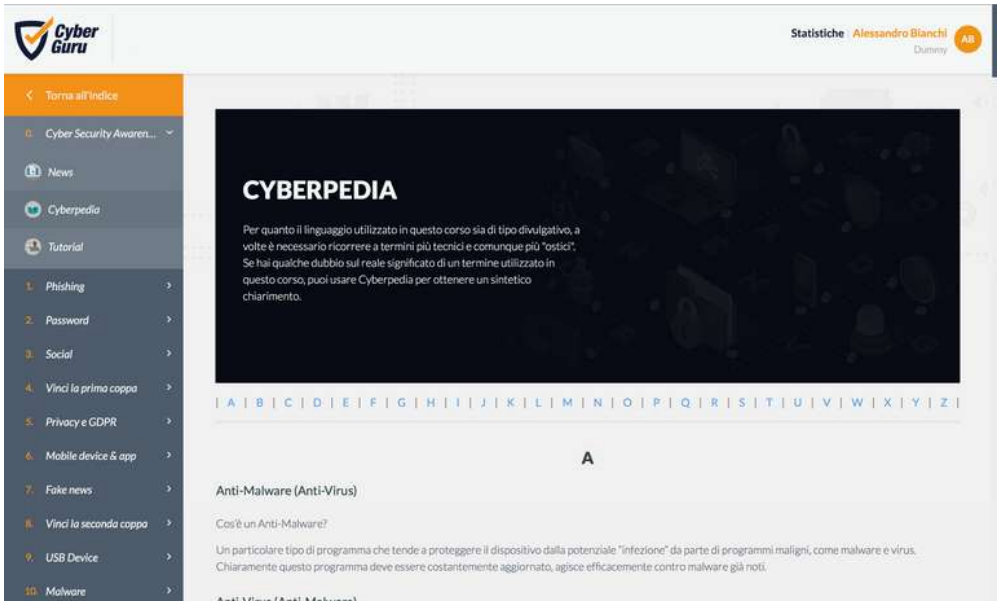
Tutte le statistiche vengono fornite nel pieno rispetto della Privacy e della tutela dei dati personali. Ogni partecipante può vedere solo i propri indicatori, rapportati al team e all'organizzazione, e i dati aggregati per team e per organizzazione, visibili ai team leader. L'unica statistica personale visibile a tutti è il cosiddetto medagliere, che evidenzia solo i meriti di coloro che hanno profuso il massimo impegno.

Statistiche e privacy

CYBERPEDIA

Per rendere ancora più semplice la fruizione della piattaforma esiste un'ampia sezione tutorial che descrive in maniera estremamente chiara ogni unità funzionale, ricorrendo a tecniche di video animazione.

La sezione Cyberpedia consente inoltre di approfondire il significato di concetti e termini tecnici che vengono utilizzati durante il corso. Come già riferito in precedenza, il corso usa un linguaggio estremamente divulgativo che rifugge ogni ortodossia tecnologica. In alcuni casi però è necessario ricorrere a concetti e termini più tecnici, che vengono "spiegati" all'interno della sezione Cyberpedia. In alcuni casi questa sezione serve a ritrovare una terminologia di tipo tecnico a un concetto che nei contenuti del corso viene trattato in modo divulgativo.



GAMIFICATION

I test di apprendimento e di valutazione, le classifiche, individuali e di team, l'organizzazione in team, l'assegnazione di coppe e medaglie sono tutti elementi che contribuiscono a stimolare il gioco e la competizione virtuosa, rendendo il percorso formativo più coinvolgente.

La sezione Cyberpedia

CARATTERISTICHE DI CYBER GURU AWARENESS

Ogni elemento è stato progettato e realizzato per massimizzare l'efficacia del contributo formativo, minimizzando l'effetto dispersivo e annullando i costi di gestione:

.

- **LINGUAGGIO DIVULGATIVO** - Un linguaggio adatto a tutti e lontano da ogni forma di ortodossia tecnologica
- **SESSIONI BREVI** - Organizzazione per brevi lezioni e moduli auto-consistenti, all'interno di un percorso integrato
- **MATERIALE MULTIMEDIALE** – Uso di video-lezioni, centrate sulla figura dell'attore-coach, supportato da elementi di animazione video
- **APPROCCIO INTERATTIVO** - Un'alternanza continua tra esposizione a brevi contenuti formativi e test di apprendimento e valutazione
- **PERVASIVE GAMIFICATION** - Una struttura per team in competizione fra loro, con utilizzo di classifiche e premi virtuali
- **REPORTISTICA EFFICACE** - Una serie di report che definiscono la partecipazione a livello qualitativo e quantitativo
- **STUDENT CARING** - Un sistema automatizzato che stimola l'utente a partecipare attivamente con delle mail mirate
- **LEVA INDIVIDUALE** - La piattaforma fa leva sui benefici che il partecipante ottiene nella sua sfera individuale
- **CONTINUOS TRAINING** - Contenuti brevi e diluiti nel tempo per mantenere sempre l'attenzione elevata sulle minacce (12/24/36 mesi)
- **USER EXPERIENCE** - La piattaforma è stata progettata per garantire la massima facilità di utilizzo e l'ottimale fruizione dei contenuti.

Massima efficacia

IL PRIMO LIVELLO FORMATIVO

Benché ogni modulo sia auto-consistente, la sequenza dei 12 moduli formativi è stata studiata per produrre dei “naturali” richiami ad argomentazioni già affrontate in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

PHISHING

Il PHISHING è la più comune tecnica di attacco utilizzata dai criminali Cyber e utilizza la mail come principale veicolo di diffusione, anche se si va estendendo velocemente ad altri canali, come i più popolari canali di messaggistica e i canali social. È particolarmente subdolaperché basata su un inganno, con cui si cerca di indurre la potenziale vittima a compiere un’azione che consente al criminale di sferrare il suo attacco. Questo modulo formativo fornisce gli elementi cognitivi per riconoscere un attacco PHISHING e per adottare le necessarie contromisure.

PASSWORD

Uno dei pilastri della Cyber Security è rappresentato dalla PASSWORD, la chiave di accesso a tutte quelle risorse informatiche a cui si deve garantire un accesso sicuro e riservato. La gestione delle proprie PASSWORD diventa quindi un elemento basilare delle strategie difensive, della persona e dell’organizzazione. Questo modulo formativo fornisce gli elementi cognitivi necessari ad una gestione sicura delle PASSWORD, mettendole al riparo da tentativi di violazione che potrebbero avere conseguenze disastrose.

Moduli primo livello

SOCIAL MEDIA

I SOCIAL MEDIA rappresentano una nuova modalità di socializzazione basata sulle ampie possibilità che la tecnologia digitale mette oggi a disposizione. Ma allo stesso tempo sono anche fattori di rischio, dove si può arrivare a compromettere sia la privacy delle persone sia la sicurezza dei sistemi delle organizzazioni. Questo modulo fornisce gli elementi cognitivi per utilizzare in modo consapevole questi strumenti, proteggendo la persona e l'organizzazione dai rischi che la condivisione in rete di contenuti individuali e professionali può generare.

PRIVACY & GDPR

L'introduzione del nuovo regolamento europeo sulla protezione dei dati aumenta la sensibilità delle organizzazioni rispetto alla PRIVACY e alla protezione dei dati sensibili. Al di là dei ruoli specifici, è importante che tutti i membri di un'organizzazione acquisiscano maggiore sensibilità rispetto alla protezione dei dati. Questo modulo fornisce gli elementi cognitivi per assumere un atteggiamento proattivo rispetto alla protezione dei dati, e per contribuire alla conformità dell'organizzazione rispetto alle nuove norme europee.

MOBILE & APP

I DEVICE MOBILI, soprattutto Smartphone e Tablet, sono strumenti che diventano ogni giorno più critici e che rappresentano la massima espressione della rischiosa sovrapposizione tra dimensione personale e professionale. Questo modulo fornisce gli elementi cognitivi per utilizzare i dispositivi mobili, siano essi personali o professionali, in modo consapevole, abilitando buone pratiche che siano in grado di aumentare il livello di sicurezza e di protezione dei dati.

Moduli primo livello

FAKE NEWS

Le FAKE NEWS sono articoli redatti con informazioni inventate o semplicemente distorte, che hanno lo scopo di disinformare. Sono un fenomeno pericoloso, che se non controllato può avere ripercussioni negative sia per l'individuo sia per le organizzazioni. L'argomento viene spesso trattato dal punto di vista sociale e politico, ma ha anche una implicazione diretta con la Cyber Security. Questo modulo formativo fornisce gli elementi cognitivi necessari a riconoscere una Fake News, attivando alcuni processi di indagine che aiutano a sviluppare un atteggiamento corretto su qualsiasi informazione acquisita in rete.

MEMORIE USB

Le MEMORIE USB, e comunque tutte le memorie esterne, possono diventare un punto critico rispetto alla necessità di proteggere le informazioni riservate, ed è per questa ragione che sono spesso oggetto di specifiche policy. Questo modulo formativo fornisce gli elementi cognitivi per riconosce tutti i rischi associati alle memorie esterne, abilitando buone pratiche per evitare di incorrere in fenomeni di sottrazione di dati.

EMAIL SECURITY

La MAIL è uno strumento sempre più importante, che nella vita professionale assume un ruolo centrale e particolarmente critico. Attraverso le MAIL vengono scambiate informazioni sensibili e quindi l'aspetto della sicurezza non può essere sottovalutato. Questo modulo formativo fornisce gli elementi cognitivi per le mail e le informazioni in esse contenute.

Moduli primo livello

MALWARE & RANSOMWARE

I MALWARE in generale e il RANSOMWARE in particolare hanno conquistato velocemente gli onori della cronaca, mettendo in evidenza tutta la loro pericolosità. Le persone devono comprendere che i software anti-virus non garantiscono la protezione totale rispetto a questi programmi maligni. Questo modulo formativo fornisce gli elementi cognitivi per ridurre il rischio di cadere vittima di questa particolare tipologia di software e per limitare le conseguenze negative in caso di violazione.

WEB BROWSING

La NAVIGAZIONE nel WEB presenta molti rischi e in quella che ormai sembra quasi un'attività scontata si presentano molti aspetti critici. Una buona conoscenza di alcune caratteristiche peculiari dei siti Web e dei browser può aiutare a ridurre notevolmente il livello di rischio. Questo modulo formativo fornisce gli elementi cognitivi su come navigare nel WEB in sicurezza.

CRITICAL SCENARIOS

Nell'interazione con il Cyber Spazio, esistono alcuni scenari critici: l'uso delle piattaforme Cloud, il viaggio di piacere o di affari, piuttosto che l'uso delle piattaforme di e-commerce, sia in ambito B2B che B2C. Sono scenari che risultano particolarmente esposti alla possibilità di subire attacchi da parte dei criminali Cyber, con rischi sia sul piano individuale sia sul piano professionale. Questo modulo vuole fornire elementi essenziali di consapevolezza che aiutano a comprendere le minacce, spesso sottovalutate, che sono collegate a questi particolari scenari di utilizzo delle tecnologie digitali.

Moduli primo livello

SOCIAL ENGINEERING

Il social engineering, o ingegneria sociale, è la madre di tutte le strategie di attacco Cyber. È una strategia che punta sull'inganno e sulla manipolazione psicologica per perseguire finalità truffaldine. Per rendere più efficace l'attacco, il nucleo di questa strategia è costituito dall'acquisizione di informazioni sulla vittima designata. Questo modulo fornisce elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli precedenti.

Moduli primo livello

IL SECONDO LIVELLO FORMATIVO

Benché ogni modulo sia auto-consistente, la sequenza dei 12 moduli formativi è stata studiata per produrre dei “naturali” richiami ad argomentazioni già affrontate in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

CLEAN DESK

Mantenere una particolare attenzione verso la propria postazione di lavoro, evitando di lasciare informazioni critiche o addirittura sensibili nella disponibilità di persone non autorizzate ad accedervi, è un elemento basilare per garantire la sicurezza delle informazioni, la protezione dei dati, e quindi anche il rispetto delle normative sulla privacy. Questo modulo oltre a fornire dei suggerimenti di ordine pratico, richiama concetti come quello della data protection e della privacy, anche in ottica GDPR.

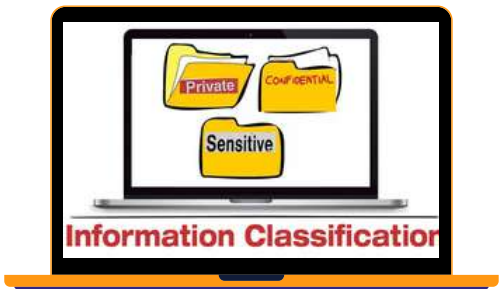
PERSONAL IDENTIFIABLE INFORMATION

Si torna a parlare di dati personali, quelli che consentono di identificare la persona, ponendo l’attenzione su di essi e sui rischi che si possono correre se non gli viene data la giusta importanza. Questo modulo, oltre a richiamare l’importanza della tutela del dato personale in un’ottica GDPR, pone l’attenzione sui dati personali dell’utente stesso, tracciando alcuni scenari molto pericolosi per la sua sicurezza e per quella della sua organizzazione. L’obiettivo primario è quello di aumentare la sensibilità dell’utente sulla necessita di tutelare questa particolare tipologia di dati.

Moduli
secondo livello

INFORMATION CLASSIFICATION

La classificazione delle informazioni è uno dei fattori chiave nella gestione della sicurezza delle informazioni, ma è anche uno dei fattori meno compresi dagli utenti e spesso vissuto come un'inutile imposizione. Eppure, oggi la classificazione delle informazioni è diventata basilare per il rispetto di standard e normative che riguardano la protezione dei dati. Questo modulo, oltre a spiegare il significato e le motivazioni che spingono le organizzazioni a sviluppare processi di classificazione, cerca di far comprendere quanto sia importante adeguare i propri comportamenti in questa direzione.



IoT DEVICE

Siamo sempre più interconnessi e lo saremo sempre di più. L'evoluzione tecnologica ci sta portando verso l'interconnessione totale, che non riguarda più solo le persone, ma anche le cose. Quello che qualche anno fa si sarebbe considerato uno scenario fantascientifico, si sta concretamente realizzando sotto i nostri occhi. E questo non riguarda solo la dimensione professionale, ma anche la dimensione privata degli utenti. Elettrodomestici, telecamere, dispositivi indossabili, automobili sempre più intelligenti, anche le cose sono destinate a comunicare sempre di più. La questione si fa per certi versi sempre più affascinante, per altri sempre più inquietante. Ogni dispositivo interconnesso, se non gestito correttamente, diventa un punto di potenziale vulnerabilità per la sicurezza. Questo modulo ci spiega come relazionarci con questo scenario, proponendo comportamenti adeguati che non compromettano il livello di sicurezza della persona e dell'organizzazione.

Moduli secondo livello

AWAY FROM THE OFFICE

Questo modulo vuol far riflettere sui rischi Cyber che incontriamo fuori dalle “rassicuranti” mura del nostro ufficio, soprattutto quando abbiamo la necessità di relazionarci con la nostra dimensione professionale e quindi di connetterci e interagire con i sistemi della nostra organizzazione. L’analisi riguarda i principali punti di vulnerabilità che si incontrano in questa dimensione meno protetta e come si possono mitigare i rischi con comportamenti adeguati che riflettono una maggiore consapevolezza.

SPEAR PHISHING

Si torna a parlare di Phishing richiamando concetti già affrontati in precedenza, partendo dal presupposto che il nostro utente abbia con i precedenti moduli maturato un livello di conoscenza di base per approfondire alcuni argomenti e aumentare la sua capacità di riconoscere un attacco Phishing. In questo modulo, focalizzato sulla necessità di riconoscere un attacco di Spear Phishing e quindi una tecnica sofisticata che colpisce uno specifico individuo o uno specifico gruppo di individui, si pone l’accento su quelle tecniche, che hanno lo scopo di collezionare informazioni sensibili attraverso l’inganno.

SMISHING & VISHING

Un'altra particolare tecnica di Phishing che colpisce attraverso i sistemi di messaggistica come WhatsApp, Messenger, Telegram, e SMS. Questo modulo, attraverso una serie di esempi concreti, vuole far comprendere all’utente, come anche i sistemi di messaggistica, per certi versi considerati “SICURI”, possono nascondere particolari insidie. Mettendo in evidenza come un comportamento non adeguato e poco attento, oltre a mettere in pericolo la nostra sicurezza, e quella della nostra rete relazionale.

Moduli secondo livello

PHONE SCAM

Esiste una relazione sempre più stretta tra le truffe telefoniche e le truffe Cyber. Spesso le due tecniche si integrano in una strategia di attacco più complessa e sofisticata: la truffa telefonica è il presupposto che viene spesso utilizzato per acquisire informazioni che poi diventano la base per colpire nella dimensione Cyber. Questo modulo pone l'attenzione su alcuni casi concreti per aumentare il livello di consapevolezza verso alcuni rischi specifici.

SNEAKY PHISHING

Questo modulo affronta un'ulteriore evoluzione degli attacchi phishing, analizzando una tecnica che vuole compromettere il doppio livello di autenticazione, sviluppato proprio per aumentare il livello di sicurezza di sistemi e applicazioni. Anche il doppio fattore di autenticazione contiene punti di vulnerabiltà strettamente correlati con il fattore umano e quindi con i comportamenti inconsapevoli degli utenti.

BLUETOOTH & WIFI

Questo modulo focalizza la sua attenzione su due componenti tecnologiche che sono necessarie per garantire la connessione in movimento e quindi la mobilità delle persone. Sono due componenti strategiche per la trasformazione digitale e per l'innovazione, ma contengono delle insidie che possono essere controllate con un atteggiamento consapevole da parte degli utenti nel loro uso.

Moduli secondo livello

DATA PROTECTION

Si torna a parlare di protezione dei dati, con un accezione che riguarda la sicurezza, e più strettamente la Privacy e la relazione con le varie normative di qualità e di sicurezza delle informazioni, in modo particolare con il GDPR. Questo modulo può essere considerato un richiamo “annuale” del modulo Privacy & GDPR, in una logica di formazione obbligatoria, anche se presenta contenuti originali e più sofisticati rispetto a quelli trattati nel primo livello.

SOCIAL ENGINEERING 2

Alla fine di ogni livello (annualità) si torna a parlare di Social Engineering, e quindi di tecniche di attacco che usano l’inganno e la manipolazione psicologica come base per raggiungere i loro scopi fraudolenti. Questo modulo, prendendo spunto da alcuni esempi tratti dalla realtà, fornisce ulteriori elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli del secondo livello.

Moduli secondo livello

IL TERZO LIVELLO FORMATIVO

Benché ogni modulo sia auto-consistente, la sequenza dei 12 moduli formativi è stata studiata per produrre dei “naturali” richiami ad argomentazioni già affrontate in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

PRIVACY

Torniamo a parlare di Privacy approfondendo l’argomento e soprattutto mettendo in evidenza il valore della stessa e l’importanza di tutelarla. L’obiettivo di questo modulo è quello di fornire gli strumenti cognitivi per comprendere il fatto che l’uso delle tecnologie digitali, del Web e dei Social hanno un prezzo in termini di perdita di Privacy. Un atteggiamento consapevole in questo ambito ci può consentire di vivere in modo equilibrato il rapporto con l’innovazione, senza per questo pagare un prezzo eccessivamente alto in termini di riservatezza.

SOCIAL & CYBERBULLYING

Si parla di Social per affrontare una particolare emergenza sociale, quella del Cyberbullismo. Come sempre i nostri moduli tendono a calarsi in una duplice dimensione, quella personale e quella professionale, spesso fortemente sovrapposte tra di loro. Questo modulo affronta quindi un tema che sembra dedicato alla sfera strettamente personale con una caratterizzazione esclusivamente sociale e culturale. In realtà, oltre a fornire una sensibilizzazione di carattere culturale, vedremo come la sottovalutazione di alcuni fenomeni può avere ripercussioni anche dal punto di vista della sicurezza, e può comportare anche danni legali o di immagine verso la propria organizzazione.

Moduli terzo livello

LEGAL ASPECT

In questo modulo affrontiamo alcuni aspetti legali correlati con l'uso inconsapevole delle tecnologie digitali. Violazione del copyright, mancato rispetto delle normative, uso non legittimo di prodotti software, diffamazione, sono solo alcuni degli esempi concreti del rischio di commettere reati che possano avere un impatto negativo sulla persona e sull'organizzazione.

REAL SCAM 1

In questo modulo presentiamo alcuni casi reali di truffe avvenute nella dimensione Cyber. L'obiettivo primario è quello di favorire il processo di acquisizione di consapevolezza, realizzando proprio quanto possa essere concreto il pericolo. Nel modulo verranno inoltre richiamate alcune buone pratiche, che avrebbero evitato di diventare vittime di una truffa.

REAL SCAM 2

Ancora casi reali e ancora buone pratiche. Si prosegue sulla falsa riga del modulo precedente per fornire nuovi elementi di identificazione tempestiva rispetto a truffe concrete che si diffondono a macchia d'olio, proprio per l'assenza di atteggiamenti consapevoli.

Moduli terzo livello

MALWARE

ITorniamo a parlare di Malware nell'ottica di mantenere elevata l'attenzione sui rischi che si corrono di infettare i propri dispositivi e di conseguenza quelli della propria organizzazione con comportamenti incauti. Con questo modulo si vogliono fornire maggiori informazioni su questo specifico argomento, aumentando la capacità di prevenire e di identificare attacchi che sono spesso solo l'inizio di un processo che può provocare molti danni. Nell'affrontare l'argomento si tiene quindi conto della crescita in termini di cultura Cyber che l'utente ha fatto nel suo percorso formativo.

E-COMMERCE

Questo modulo focalizza l'attenzione su un tema che è stato soltanto introdotto nel primo livello formativo. Il tema è particolarmente delicato, perché i rischi aumentano, così come l'entità dei potenziali danni, quando un'attività è direttamente collegata con un flusso di denaro, come nel caso del commercio elettronico. Affrontiamo il tema a 360° considerando le varie tipologie di commercio elettronico, da quelle B2C a quelle B2B, che hanno maggiore impatto rispetto all'organizzazione.

HOLIDAY & BUSINESS TRIP

Questo modulo focalizza l'attenzione su un tema che è stato soltanto introdotto nel primo livello formativo. Il tema riguarda le vacanze e i viaggi di lavoro, perché la nostra vulnerabilità Cyber aumenta sempre quando affrontiamo una situazione di questo tipo. Affrontiamo il tema cercando di coprire l'intero ciclo del viaggio – dalla pianificazione al rientro a casa o in ufficio – osservando tutti i rischi che si presentano in ognuna delle fasi.

Moduli terzo livello

CYBER HYGIENE

Mantenere i dispositivi in un corretto stato di igiene, aiuta a ottenere maggiori risultati in termini di produttività, ma soprattutto comporta una riduzione dei rischi sulla sicurezza delle informazioni. Dobbiamo sempre mantenere una strategia di corretta manutenzione dei dispositivi, che comprenda anche la cura del contenuto, e quindi dei dati. Questo modulo fornisce una serie di buone pratiche su come mantenere una corretta igiene dei nostri dispositivi e soprattutto un controllo sui dati che possono essere acceduti attraverso di essi

BACKUP & RESTORE

Avere una corretta strategia di salvataggio e di recupero dei dati consente alle persone e di conseguenza alle organizzazioni, di mettersi al riparo dal rischio di subire danni a fronte di un attacco Cyber che ha avuto successo. Questo modulo vuole creare consapevolezza rispetto a quella che può essere considerata a tutti gli effetti un'arma di difesa, che ci permette di evitare che il nostro dispositivo diventi oggetto di un riscatto, come avviene nei casi di attacco Ransomware, o di trovarci nella condizione di aver perso dati importanti che a fronte di un banale evento tecnologico.

BEST PRACTICE

Tutto il percorso formativo è centrato sulle buone pratiche, intese come comportamenti virtuosi in grado di mitigare i rischi Cyber. Questo modulo sintetizza il concetto andando a porre l'accento su 12 buone pratiche che possono concretamente essere di aiuto nel ridurre il rischio Cyber.

Moduli terzo livello

SOCIAL ENGINEERING 3

Alla fine di ogni livello (blocco 12 moduli) si torna a parlare di Social Engineering, e quindi di tecniche di attacco che usano l'inganno e la manipolazione psicologica come base per raggiungere i loro scopi fraudolenti. Questo modulo, prendendo spunto da alcuni esempi tratti dalla realtà, fornisce degli ulteriori elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli del terzo livello.

Moduli terzo livello

IL PROCESSO DI SVILUPPO

LA QUALITA' DI CYBER GURU AWARENESS

La qualità di Cyber Guru Awareness è garantita da un processo di sviluppo e aggiornamento particolarmente efficace e attento al particolare. La necessità di rendere accessibile a tutti una formazione che riguarda argomentazioni che presentano un background di tipo tecnico e che fino a ieri rappresentavano un'esclusiva degli specialisti di Cyber Security, richiede la massima cura di ogni elemento del processo e il ricorso alle metodologie più avanzate dal punto di vista pedagogico ed educativo.

PIATTAFORMA DI EROGAZIONE

Prima di approfondire il processo, poniamo l'attenzione sulla piattaforma di erogazione, che è uno dei punti di forza della proposta Cyber Guru Awareness.

La piattaforma di erogazione è basata sul framework di e-Learning Moodle, uno strumento didattico, con accesso ed utilizzo interamente dal web e che si basa su modelli responsive e quindi pienamente accessibili da qualsiasi dispositivo, inclusi i dispositivi mobili.

Moodle è il framework di e-learning più diffuso al mondo, in particolar modo nelle Istituzioni accademiche e scolastiche: oltre 1150 organizzazioni di vario genere e tipologia di 81 paesi del mondo hanno installato la piattaforma Moodle per gestire le attività di e-Learning; in Italia è utilizzata da moltissime organizzazioni e da gran parte delle istituzioni scolastiche ed universitarie.

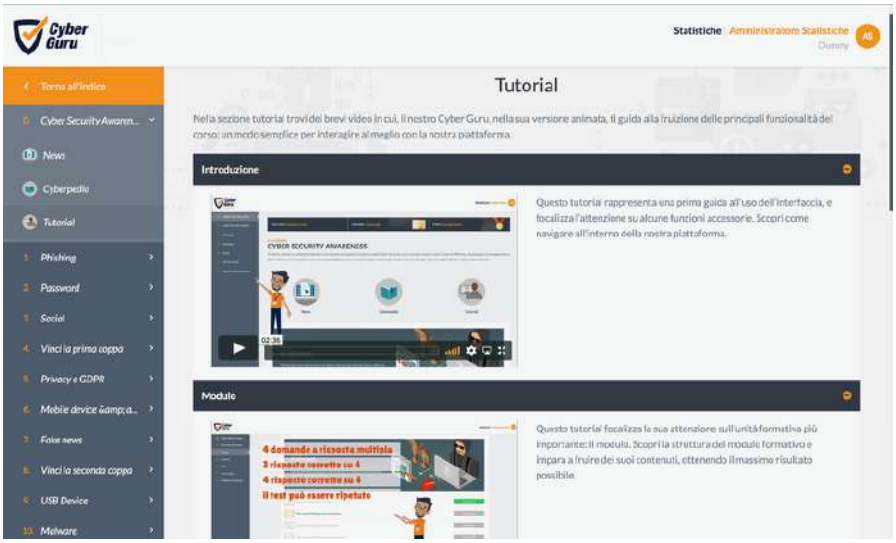
USER INTERFACE

Per la realizzazione della piattaforma sono stati adottati i più attuali e consolidati paradigmi di progettazione orientati a garantire la massima facilità di utilizzo da parte di un parco utenti estremamente eterogeneo.

e-learning Moodle

Le soluzioni di user experience introdotte (e validate su un apposito campione di utenti) hanno posto al centro l'obiettivo di supportare l'utente nell'avanzamento del proprio percorso formativo a partire da un impianto di fruizione verticale (modulo > lezione > test di verifica) pensato per minimizzare l'effort cognitivo e garantire un agevole approdo alla didattica; gli utenti possono quindi facilmente accedere ai contenuti loro proposti avanzando tra moduli e lezioni e, in un'ottica di continuità e semplicità, riprendere velocemente il percorso formativo eventualmente interrotto bypassando le informazioni a corredo dell'esperienza.

Sebbene la piattaforma proponga un modello di fruizione estremamente semplice, gli utenti hanno a disposizione dei videotutorial per meglio comprendere le diverse meccaniche e le funzionalità.



La piattaforma può inoltre giovarsi di un "linguaggio" visivo e interattivo che, incentrato su codici colore (semaforo: verde, giallo e rosso) e su comportamenti della pagina, comunica con l'utente con chiarezza e precisione, stabilendo un "dialogo" che riduce via via la quantità e affina la qualità dei messaggi man mano che l'utente si misura con il percorso formativo.

Per garantire continuità e coerenza alla didattica è stata sviluppata una piattaforma fruibile con comodità da tutti i dispositivi e le cui cromie, il cui corredo iconico e i cui artwork conferiscono infine freschezza e modernità alla user interface, agendo da ulteriori elementi di facilitazione nel percorso di comprensione e interazione con il contesto.

User interface

IL PROCESSO DI SVILUPPO DELLE PIATTAFORMA

Di seguito una descrizione delle principali fasi del processo di produzione dei contenuti della piattaforma Cyber Guru Awareness:

- **Definizione dei contenuti** – è gestita dal Comitato tecnico-scientifico di Cyber Guru, specialisti della Cyber Security con provata esperienza e in possesso di tutte le certificazioni necessarie. Il comitato seleziona ed elabora i contenuti con un approccio specialistico, propone e definisce gli argomenti selezionando il materiale di base.
- **Trasformazione dei contenuti** – è la parte del processo in cui i contenuti specialistici si trasformano in contenuti di carattere divulgativo, assumendo la forma dello schema con cui vengono strutturate le lezioni (conoscenza, approfondimento, best practice). Esperti di comunicazione, con una provata esperienza nel settore IT e IT Security, si occupano di questa fase.
- **Multimedialità** – gestiti da esperti della comunicazione multimediale, i contenuti subiscono un primo adattamento alle forme e ai linguaggi video.
- **Formazione** – gestiti da esperti della formazione e condotta con la collaborazione incisiva del Dipartimento di Scienza della Formazione dell'Università di Roma Tre, i contenuti vengono ulteriormente adattati rispetto ai criteri più avanzati delle scienze pedagogiche ed educative, con lo scopo di renderli più efficaci e coinvolgenti possibile.
- **Sceneggiatura** – è la prima fase della produzione video, in cui i contenuti prendono la forma di dialoghi e di indicazioni per la fase di post-produzione. Questa fase viene gestita con la collaborazione di esperti della produzione video e multimediale.
- **Produzione Video** – include tutte le fasi di produzione e post-produzione necessarie per dare ai contenuti la forma definitiva e renderli disponibili al processo di revisione. Gestita da professionisti della produzione video e multimediale.
- **Revisione contenuti** – tutte le entità coinvolte verificano la qualità del processo di produzione dei contenuti e l'efficacia del risultato ottenuto.
- **Rilascio** – è la fase in cui i contenuti si strutturano definitivamente in lezioni, test, documenti di approfondimento, e quindi nel modulo formativo.

Produzione contenuti

INVESTIRE SUL FATTORE UMANO PER GARANTIRE LA CYBER SECUIRTY

Cyber Guru Awareness

www.cyberguru.it
contatti@cyberguru.it
Numero verde 800.741.423