

Cyber Guru Phishing è una soluzione innovativa, in **funzione AntiPhishing**, che produce risultati efficaci grazie alla sua particolare metodologia di **training on the job** e alle caratteristiche di **automazione e machine learning**.

Rivolta al **personale non specialistico** delle organizzazioni pubbliche e private, Cyber Guru Phishing consente di mantenere “allenata” la più importante delle caratteristiche difensive umane: la **prontezza**,



Cyber Guru Phishing, basato sulla tecnologia leader **CybeReady**, si propone come la naturale integrazione ai programmi formativi della linea Cyber Guru, aumentando la reattività dell’individuo di fronte a questa tipologia di attacchi.

Considerando che i maggiori pericoli per la sicurezza delle organizzazioni sono “in agguato” nelle caselle e-mail dei loro dipendenti e collaboratori, le simulazioni di attacco Phishing di Cyber Guru Phishing, “personalizzate” sulla base delle caratteristiche peculiari dell’organizzazione, preparano dipendenti e collaboratori a modificare i comportamenti e a reagire con prontezza ad attacchi inattesi, e quindi **ad essere pronti a tutto**.

## CYBER GURU PHISHING

- usa una metodologia di **on-going training** che consente di mantenere in allenamento la “prontezza” di ogni singolo dipendente e di sviluppare la sua capacità di reagire agli attacchi realizzati con le tecniche di phishing;
- invia **e-mail di phishing** in modo continuativo a tutti i dipendenti di un’organizzazione, utilizzando simulazioni di scenari di attacco diversi (inclusi spray e spear phishing) e livelli di inganno via via più sofisticati;
- consente una **personalizzazione degli attacchi** con una granularità che arriva al **singolo utente**, una personalizzazione che può essere anche eseguita in automatico del sistema, grazie a tecniche di **machine learning**;
- modifica costantemente le **strategie di simulazione** sulla base dei comportamenti degli individui, sfruttando la capacità di apprendimento “guidata dai dati”;
- predispose pagine di “atterraggio”, nelle quali il dipendente che cade nell’inganno riceve un **contenuto formativo “leggero”** ed adattato rispetto alla tipologia di attacco subito, corredato da video informativi sul phishing;
- produce un **report mensile** che esprime la mappa del rischio phishing e soprattutto il miglioramento indotto da questa strategia di allenamento.



contenuti  
multimediali



linguaggio  
divulgativo



architettura in  
cloud



personalizzazione  
per utente



organizzazione  
per gruppi

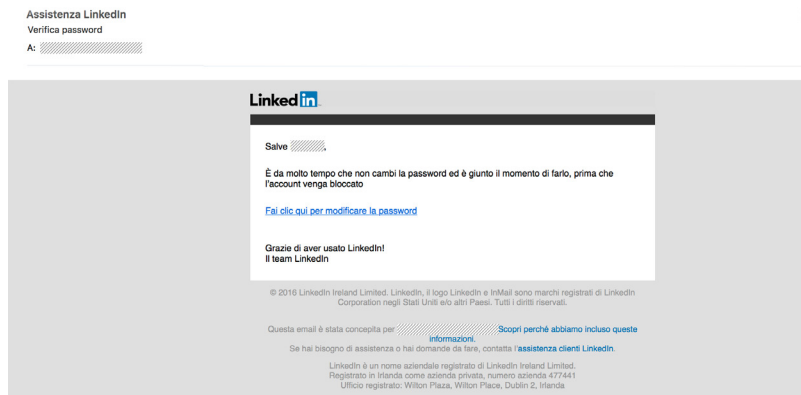


automazione &  
machine learning

## CONTENUTI CREDIBILI

I contenuti delle mail vengono progettati e realizzati per risultare **credibili ed efficaci**. I contenuti possono essere di tipo “massivo”, come nel caso dello spray phishing, oppure personalizzati sulle peculiarità dell’organizzazione cliente, come nel caso dello spear phishing.

La **personalizzazione** si spinge fino ad adattare le tipologie di attacco e le frequenze di invio, alle peculiarità del singolo utente, e alla sua tendenza a cadere o meno nell’inganno.



*LinkedIn non ha chiaramente nulla a che vedere con questi tentativi, anzi è un'azienda che si adopera costantemente per rafforzare la Cyber Awareness. I criminali Cyber sfruttano però la notorietà dei brand più famosi per rendere più credibili e quindi più efficaci le loro mail.*

## SMART TRAINING



### Attenzione, simulazione di un attacco reale

Hai fatto clic su un link in un'e-mail che simula un vero attacco e che ultimamente è stata messa in circolazione; un'e-mail simile potrebbe presto arrivare nella tua casella di posta in entrata

**Annotta questi segnali sospetti**

- Non riconosci assolutamente il mittente. Non fidarti quando il mittente è sconosciuto
- L'e-mail non è indirizzata a te direttamente e sembra essere di massa
- La minaccia contenuta nell'e-mail sta tentando di metterti pressione affinché tu faccia clic sul collegamento
- L'immagine del file nasconde un collegamento malevolo nel tentativo di aggirare i sistemi di protezione dei dati

**90 secondi di Phishing**

Questa email è stata inviata dal settore sicurezza Informazioni

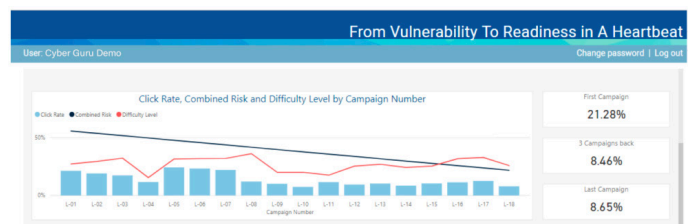
I contenuti delle mail vengono progettati e poi realizzati per risultare **credibili ed efficaci**.

Quando l’utente cade nell’inganno e clicca sul link proposto, viene indirizzato verso un **contenuto formativo** che descrive sinteticamente l’attacco subito e mette a disposizione un video formativo personalizzato sulle caratteristiche specifiche dell’attacco.

Si tratta di un contenuto formativo leggero, studiato per **favorirne la fruizione ed evitare impatti** eccessivi sulle attività lavorative.

## REPORTISTICA EFFICACE

La reportistica fornita su base mensile ha l’obiettivo di **evidenziare il livello di rischio** e l’efficacia del percorso formativo. La reportistica consente anche di **mettere in evidenza i punti di debolezza** di fronte ad eventuali attacchi e quindi di indirizzare interventi formativi più mirati e approfonditi.



## SOLUZIONE MULTILINGUA

Le simulazioni sono realizzate in 32 lingue diverse, tra cui in lingua italiana, per rispondere alle esigenze anche di aziende che hanno sedi, dipendenti e collaboratori in più di un paese. I contenuti in lingua italiana vengono realizzati da specialisti “madre lingua, così da risultare credibili e professionali.



[www.cyberguru.it](http://www.cyberguru.it)  
[contatti@cyberguru.it](mailto:contatti@cyberguru.it)

