FutureTouch

Cyber Security Awareness

Clusit
Associazione Italiana per la Sicurezza Informatica

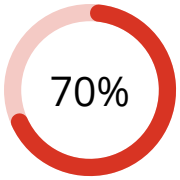
Corso di Cyber Security Awareness

Presentazione Del Corso

- La sicurezza informatica inizia con la consapevolezza
- Navigazione Web
- E-mail
- Proteggere la propria Privacy
- Social Network
- Gestione delle Password
- Protezione informazioni cartacee
- Ingegneria Sociale
- Proteggi i tuoi dati con il backup
- Decalogo
- Attestato di frequenza

Individuiamo le vulnerabilità di qualsiasi sistema informatico.

La nostra missione è sfruttare l'AI per un approccio innovativo alla cybersecurity: semplice, sicuro e accessibile.



Imprese che hanno subito almeno un attacco nel 2023

Gli attacchi hacker sono le rapine del mondo digitale, nel 2023 hanno causato $6.000 miliardi di danni nel mondo, il 6% del PIL globale, colpendo tutti: le grandi istituzioni, la PA, ma soprattutto le PMI, perché meno protette e quindi più facili da attaccare.

Attacchi gravi dovuti a errori umani

L'essere umano è l'anello debole della catena di sicurezza. Per questo motivo testiamo sia i sistemi informatici (reti, siti, app, dispositivi), sia il fattore umano (test anti-phishing).
Un approccio veloce, facile da usare, non richiede installazione e individua anche le minacce più recenti.

PMI che non impiegano personale specializzato IT

Le minacce informatiche crescono annualmente di oltre il 15% e le risorse umane specializzate sono scarse e non sono sufficienti a coprire le esigenze di sicurezza

EXTENDED VULNERABILITY ASSESSMENT

Testiamo qualsiasi sistema informatico (es., web, app, IoT), eseguendo vulnerability assessment e penetration test veloci e accurati.

ANTI-PHISHING

Simula attacchi di phishing e scopre se dipendenti e collaboratori sono in grado di riconoscere un attacco informatico.

CRI - THREAT INTELLIGENCE

Scopri se i dati, le password e le informazioni della tua azienda sono già stati sottratti e disponibili online

SICURO E CERTIFICATO

È sicuro al 100%, i report dei test sono qualificati CEH e validi ai fini della certificazione ISO 27002, 9001 ecc.

FutureTouch

ANTI-PHISHING

L’attività Anti-Phishing prevede una serie di test in ambiente protetto (tentativi di Phishing senza conseguenze dannose per l’utente) per il personale aziendale operante con la strumentazione elettronica in dotazione, attraverso l’invio casuale di e-mail di Phishing.

I test sono progettati con l’intento di mettere alla prova le competenze informatiche delle risorse umane dell’azienda attraverso messaggi a difficoltà crescente, ovvero attraverso e-mail o SMS di Phishing simulato via via meno riconoscibili dall’utente che li riceve.

UN SEMPLICE TEST CHE SALVA L'AZIENDA

Il funzionamento è molto semplice, basta inserire l’elenco degli indirizzi e-mail o numeri telefonici da testare ed il gioco è fatto: il programma invierà periodicamente e-mail di phishing con difficoltà crescente a tutti gli utenti indicati dall’organizzazione.

Nel corso del periodo di test, gli utenti dovranno affrontare la sfida di ricevere e-mail sempre più accurate ed evitare di cadere nelle trappole previste al loro interno: naturalmente operiamo in un ambiente protetto, senza ricadute reali sull’azienda e nel pieno rispetto della normativa vigente.

1 PERSONA SU 10 NON RICONOSCE LE MAIL DI PHISHING

Al termine del test forniremo un resoconto che indicherà i risultati ottenuti e le capacità dell’organizzazione di far fronte ad eventi di phishing, e potrete avere accesso ad una piattaforma di e-learning interattivo. In azienda l'anello debole è sempre l'uomo, l’unica azione per rafforzare le difese è un incremento della conoscenza dei pericoli tramite formazione e training.

E-LEARNING

Nel panorama digitale attuale, le minacce informatiche non sono più una questione solo tecnica: sono un problema umano.

Il vero anello debole? ***Le persone***

Per questo abbiamo creato un percorso formativo pensato per mettere il tuo team al centro della sicurezza.

SECURITY AWARENESS CHE LASCIA IL SEGNO

Il nostro corso è molto più di un corso online: è un'esperienza smart, veloce e concreta per aumentare la consapevolezza sulle minacce digitali. I tuoi collaboratori impareranno a riconoscere phishing, malware, trappole social e altri pericoli quotidiani, con esempi reali e linguaggio comprensibile anche ai non tecnici. Il tutto online e on-demand, senza limiti di tempo. Massima flessibilità, zero scuse.

FORMAZIONE CHE FA LA DIFFERENZA RIDUCI IL RISCHIO

Al termine del corso, ogni partecipante riceverà un attestato personale, perfetto anche per le policy interne e per documentare la formazione. E sì, siamo conformi alla normativa NIS2: perché oggi la cybersecurity non è solo una buona pratica, è un obbligo. Questo significa che non solo migliori la cultura digitale in azienda, ma ti allinei subito alle nuove direttive europee, evitando multe e brutte sorprese.

Lo sapevi che la maggior parte delle violazioni parte da un errore umano? Un clic sbagliato, una password debole, una mail aperta per distrazione. La buona notizia è che si può prevenire, ma serve una formazione pensata per il mondo reale, non teoria da manuale.

Perché quando le persone sanno cosa fare (e cosa non fare), tutta l'azienda è più sicura.

FutureTouch

La routine della nostra Awareness

Step 1 — **Onboarding**
Creazione account cliente, caricamento mail, gestione categorie e set-up industry.

Step 2 — **Phishing Simulation e Assessment**
Implement the plan, collaborate across teams, and track progress.

Step 3 — **Formazione**
Video corso con durata di 3 ore , in modalità e-learning.

Step 4 — **Continuous Phishing Simulation Phishing Simulation e Assessment**
Esercitazione con 5 livelli crescenti di difficoltà, durata 3 mesi.

Step 5 — **Training continuo**
L'utente può accedere alla piattaforma di e-learning dedicata per 12 mesi.

Step 6 — **FInal Assessment**
Report dettagliato del percorso di Cyber Security Awareness effettuato.

RELOAD

FutureTouch

Template Mail

BRT Bartolini International S.p.a

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Carrefour

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Carrefour *** INGLESE ***

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Clipcetera

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Corriere – DHL Rifiuto

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Corriere – SDA Poste Italiane

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

ISTAT Report da Compilare

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

ItaliaDomani

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Kinder Offerta

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Leroy Merlin Ordine

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Leroy Merlin Solar Panels *** INGLESE ***

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

LinkedIn – ADS

Fase 1, Fase 2, Fase 3, Fase 4, Fase 5,

Template Report

Tabella riepilogativa dei risultati

670	37
E-MAIL INVIATE	PHISHING SUBITI

In breve, la situazione informatica aziendale ha un rischio critico, da migliorare il prima possibile.

La compromissione della rete informatica aziendale è infatti possibile, a causa della presenza di tentativi di phishing andati a buon fine nei primi due attacchi, cioè quelli con difficoltà di riconoscimento molto bassa e che l'utente dotato di una preparazione minima può evitare.

Tabella riepilogativa interazioni utente

	Primo attacco	Secondo attacco	Terzo attacco	Quarto attacco	Quinto attacco
Alessia Abati	1	0	0	0	0
Andrea Montanari	1	6	0	0	0
Andrea Turchi	0	3	0	0	0
Corrado Mozziconi	0	8	2	0	1
Doriano Gollini	0	2	0	0	0
Gianni Polinelli	0	2	0	0	0
Marco Morandi	1	0	0	0	0
Maria Mannoia	3	0	0	0	0
Massimo Troisi	0	2	0	0	0
Michael Bublè	1	1	0	0	0
Michele Santoro	0	0	1	0	0
Rachid Karim	2	0	0	0	0

Template Report

Risultati tecnici del test

Primo attacco

134	9
E-MAIL INVIATE	PHISHING SUBITI

Livello di difficoltà: MOLTO BASSO

Dettagli

Sono stati inviati messaggi via e-mail contenente grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.

Commento

Questo tipo di phishing è quello più semplice da individuare. Cadere vittime di questo livello di attacco, cioè subire questo tipo di phishing (es. aprendo allegati/link vistosamente sospetti), denota una preparazione assolutamente inadeguata alla strumentazione elettronica gestita dalle risorse. Attenzione, può essere sintomo dell'assenza completa di un sistema di filtraggio spam di base o di impostazioni generali di sicurezza del server di posta errate.

Templates usati

Acea Energia

BRT - Express