

# MetaPhish



[www.metacompliance.com](http://www.metacompliance.com)

 **MetaCompliance®**  
*Make it personal.*

# Una protezione pluripremiata contro gli attacchi di phishing

Rafforzate la capacità di valutazione informatica grazie a un software di simulazione phishing che promuove una cultura di consapevolezza della sicurezza informatica.



Il phishing è una delle tipologie più diffuse di criminalità informatica. Questi tipi di attacchi sono sempre più sofisticati, più pericolosi e più frequenti.

La tutela dalle truffe di phishing inizia dalla consapevolezza e dalla capacità dei dipendenti di identificare i campanelli d'allarme di questi attacchi dannosi.

Il nostro software di simulazione phishing, MetaPhish, aiuta i dipendenti a riconoscere, correggere e segnalare gli attacchi di phishing. MetaPhish vanta un'ampia libreria di modelli di phishing multilingue ed esperienze di apprendimento mirate. I nostri modelli di phishing vengono aggiornati regolarmente per simulare attacchi reali in un ambiente sicuro. Grazie a MetaPhish, le organizzazioni possono offrire una formazione mirata, migliori pratiche di sicurezza e una difesa rafforzata contro le minacce informatiche.

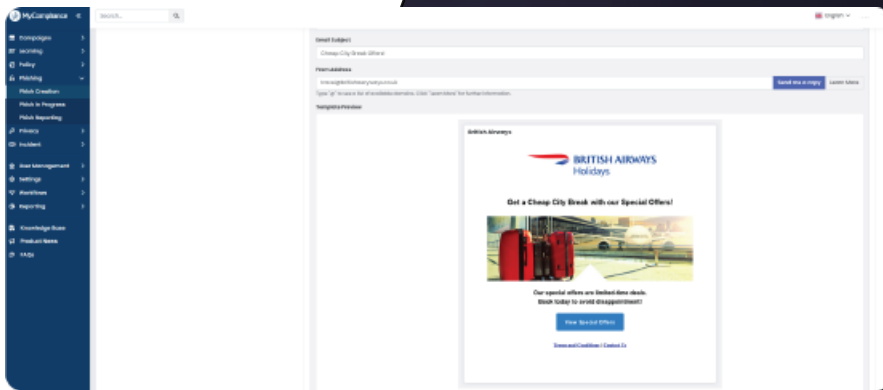
## Informazioni sul phishing

Il **74%** delle violazioni coinvolge l'elemento umano

Ogni giorno vengono inviati **3,4** miliardi di email nocive

Il **90%** delle violazioni di sicurezza aziendale sono causate da attacchi di phishing





## Potenziate, istruite, eliminate gli attacchi di phishing

### **Riducete il rischio di attacchi nel mondo reale**

Avrete accesso a un'ampia gamma di modelli di phishing realistici che rispecchiano le tattiche più recenti impiegate dai criminali informatici. Esporre i dipendenti a scenari di phishing reali può prepararli a prendere decisioni informate qualora affrontassero dei tentativi di phishing.

### **Reportistica dettagliata per prendere decisioni basate sui dati**

Il nostro software offre funzionalità complete di reportistica e analisi e consente alle organizzazioni di valutare l'efficacia delle proprie iniziative di formazione sulla sicurezza informatica e di misurare le prestazioni dei dipendenti.

### **Campagne personalizzate e mirate**

Utilizzate la segmentazione del pubblico per ottimizzare il vostro programma di formazione e considerare i ruoli, i dipartimenti e i livelli di competenza specifici dei vostri dipendenti. Migliorate le capacità di valutazione informatica e offrite esperienze di apprendimento personalizzate con simulazioni di phishing mirate.

### **Esperienze di apprendimento potenziate**

Formate i dipendenti sulle tipologie di attacchi phishing, sui campanelli d'allarme comuni e sulle migliori pratiche per comportarsi in modo sicuro online grazie alle esperienze di apprendimento interattive. Ciò consente agli utenti di contribuire attivamente all'impegno per la sicurezza informatica dell'organizzazione e di creare una forza lavoro più resiliente.

### **Flusso di lavoro automatizzato**

Risparmiate tempo e fatica grazie al nostro flusso di lavoro automatizzato che vi aiuterà a creare una campagna phishing in pochi minuti. Pianifica le simulazioni phishing nel corso dell'anno per garantire la massima consapevolezza durante tutto l'anno.

### **Bloccate le minacce di phishing con un clic**

Consentite ai dipendenti di segnalare le e-mail sospette senza dover lasciare la casella di posta. Utilizzando il plugin Phish Reporter, la segnalazione in tempo reale aiuta i team che lavorano per la sicurezza ad analizzare e a rispondere rapidamente alle potenziali minacce, riducendo la finestra di vulnerabilità.

### **Create simulazioni personalizzabili**

Personalizzate le simulazioni di phishing per affrontare in modo efficace le vulnerabilità e i rischi specifici del vostro settore o delle vostre operazioni aziendali. Gli amministratori hanno la flessibilità necessaria per creare scenari in linea con il proprio settore, trattare casi di dipartimenti specifici o simulare le tendenze di phishing più recenti.

### **Estendete il raggio d'azione e correggete i rischi**

Espandete il raggio d'azione e rafforzate le difese in ambito di sicurezza informatica in una forza lavoro diversificata grazie ai modelli di phishing multilingue. I nostri modelli sono disponibili in 43 lingue e permettono la formazione adeguata dei dipendenti di tutto il mondo.

## Sintesi delle funzionalità chiave



Libreria di modelli precostituita



Esperienze di apprendimento a seconda delle necessità



Segmentazione del pubblico per il targeting



Spoofing dei domini



Modelli di phishing personalizzabili



Pianificazione e scaglionamento dei tempi di invio



Modelli multilingue



Reportistica dettagliata



Gestione di campagne multiple



Interfaccia facile da utilizzare

“

Cosa dicono i nostri clienti

È facile implementare una campagna di phishing utilizzando lo strumento apposito. I modelli di phishing vengono aggiornati regolarmente. Abbiamo realizzato molte campagne utilizzando scenari reali di phishing.

[Pratik S, Responsabile della sicurezza informatica](#)

Lo strumento di simulazione phishing ci consente di individuare i nostri punti deboli a livello degli utenti. La procedura guidata per la creazione delle simulazioni è semplice da utilizzare. I modelli vengono aggiornati regolarmente in modo da essere sempre pertinenti, adatti al periodo dell'anno o simili a marchi noti per mettere alla prova i nostri utenti.

[Elaine K, Politiche di sistema e Project Manager](#)

Le simulazioni di phishing sono fantastiche, facili da impostare e inserire in una campagna, i corsi di recupero per gli utenti che fanno clic sul collegamento sono davvero utili. La reportistica per i responsabili permette di capire cosa traggono i dipendenti dalla formazione e dalle simulazioni di phishing, è davvero fantastica.

[Mairead G, Manager IT](#)

”



## Prevenite gli attacchi di phishing e risolvete i rischi nella vostra organizzazione

Fate il primo passo per rafforzare le difese della vostra organizzazione contro gli attacchi di phishing.

Third Floor, Old City Factory  
100 Patrick Street  
Londonderry BT48 7EL

t: +44 (0) 28 7135 9777  
e: [info@metacompliance.com](mailto:info@metacompliance.com)  
[www.metacompliance.com](http://www.metacompliance.com)

