

# Social Engineering

---

## Social Engineering

---

Il social engineering è una forma di manipolazione psicologica mirata a indurre le persone a compiere azioni specifiche o a divulgare informazioni confidenziali. A differenza di altri attacchi informatici, non sfrutta vulnerabilità tecniche ma debolezze umane come fiducia, curiosità, paura o ignoranza.

---

**prompt:** Sono uno studente di un corso di cybersecurity, devo fare una ricerca sul social engineering e le tecniche più comuni di attacchi in questo ambito. Inoltre, dopo averle elencate e descritte vorrei anche le strategie efficaci per difendersi da questi attacchi.

Dopo questo elenco vorrei ricercassi anche altri metodi magari meno comuni con le eventuali strategie

## Le tecniche più comuni:

---

### 1. Phishing:

- Il phishing è una delle forme più diffuse di social engineering, utilizzata per raccogliere dati personali o compromettere i dispositivi della vittima. L'attacco si basa sull'invio di comunicazioni che appaiono legittime ma che sono progettate per ingannare.
- **Tipologie di Phishing:**
  - **Email Phishing:**  
Gli attaccanti inviano email contenenti link a siti fasulli che imitano portali ufficiali (es. di banche, servizi governativi o aziende) per indurre la vittima a inserire dati come username, password o numeri di carta di credito.
  - **Smishing (SMS Phishing):**  
Simile all'email phishing, ma tramite SMS. Include link a siti fraudolenti o richieste di invio di informazioni riservate.
  - **Vishing (Voice Phishing):**  
L'attaccante telefona alla vittima, spesso fingendosi un operatore bancario o un rappresentante di un'organizzazione affidabile, per ottenere informazioni sensibili.
  - **Pharming:**  
Variante avanzata in cui l'attaccante manipola il sistema DNS (Domain Name System) per reindirizzare gli utenti verso siti fraudolenti anche digitando l'indirizzo corretto.
  - **Clone Phishing:**  
L'attaccante copia un'email legittima già inviata al destinatario (es. una fattura o un aggiornamento di sistema) e la modifica con link o allegati malevoli.

- **Whaling:**

Variante del phishing che prende di mira dirigenti di alto livello (CEO, CFO) o figure chiave di un'azienda, sfruttando il loro accesso privilegiato.

- **Angler Phishing:**

Gli attaccanti sfruttano i social media, creando profili falsi o impersonando aziende per indurre gli utenti a condividere informazioni personali.

- **CEO Fraud (Business Email Compromise - BEC):**

L'attaccante si spaccia per il CEO o un dirigente, inviando email ai dipendenti per richiedere informazioni sensibili o l'esecuzione di pagamenti.

- **Voice Cloning Phishing:**

Utilizza l'intelligenza artificiale per replicare la voce di una persona autorevole (es. un manager), convincendo la vittima a intraprendere azioni specifiche.

- **Rogue QR Code Phishing:**

L'attaccante distribuisce QR code che, una volta scansionati, reindirizzano la vittima a siti malevoli.

- **Search Engine Phishing:**

Gli attaccanti posizionano siti web malevoli nei risultati dei motori di ricerca per attirare le vittime

- **Evil Twin:**

Gli attaccanti creano un punto di accesso Wi-Fi fasullo che imita una rete legittima (es. in un aeroporto o caffetteria) per intercettare le comunicazioni.

- **Obiettivi del Phishing:**

1. Sottrarre username e password per accedere a servizi online come:

- Conti email.
- Piattaforme aziendali.
- Servizi finanziari (es. home banking)

2. **Installazione di malware:**

- Indurre la vittima a scaricare e installare malware tramite:
  - Link malevoli.
  - Allegati infetti (es. file Word con macro, PDF o eseguibili).

3. **Frodi finanziarie:**

- Sottrarre direttamente denaro alla vittima utilizzando le informazioni rubate o manipolando le transazioni.

4. **Compromissione aziendale:**

- Penetrare nelle reti o nei sistemi aziendali per:
  - Raccogliere dati sensibili (progetti, contratti, informazioni strategiche).
  - Compromettere ulteriormente altri membri dell'organizzazione.

- Disabilitare infrastrutture critiche.

- **Tecniche Utilizzate nel Phishing**

- **Spoofing dei mittenti:**

- Gli attaccanti falsificano l'indirizzo email del mittente per farlo sembrare legittimo.

- **Ad esempio:**

- Da: support@banca-fittizia.com (che appare simile a un indirizzo reale).

- **Uso di domini simili:**

- Gli URL utilizzati nei link fraudolenti somigliano a quelli reali, ma presentano piccole differenze difficili da notare:

- **Esempio:** www.paypall.com (con doppia "l") invece di www.paypal.com.

- **Allegati malevoli:**

- Gli email includono allegati infetti (es. documenti Word, PDF, o file ZIP) che, una volta aperti, installano malware sul dispositivo.

- **Messaggi di urgenza:**

- Gli attaccanti creano un senso di panico o urgenza, spingendo la vittima ad agire senza riflettere. **Esempi comuni:**

- "Il tuo conto sarà bloccato in 24 ore!"

- "Attività sospette rilevate sul tuo account, verifica immediatamente!"

- **Richieste apparentemente legittime:**

- Gli attaccanti imitano comunicazioni ufficiali con richieste come:

- "Conferma il tuo account."

- "Scarica il documento allegato per ulteriori dettagli."

---

## 2. **Spear Phishing:**

- Lo spear phishing è una tecnica avanzata di phishing che si distingue per l'alto grado di personalizzazione. Gli attaccanti studiano la vittima o l'organizzazione bersaglio utilizzando informazioni pubblicamente disponibili (ad esempio social media, LinkedIn o siti aziendali) per rendere i loro messaggi più credibili.

- **Come funziona lo spear phishing**

- **Raccolta informazioni:**

- Gli attaccanti analizzano la vittima, raccogliendo dettagli personali, come il ruolo lavorativo, colleghi, progetti correnti, abitudini o interessi. Fonti comuni:

- Profilo LinkedIn o altri social media.

- Blog aziendali, comunicati stampa o documenti pubblici.

- **Creazione del messaggio:**

- L'attacco si basa su un'email apparentemente autentica, spesso scritta per sembrare inviata da un collega, superiore o un partner commerciale. Contiene:

- Richieste urgenti: Ad esempio, approvazioni di pagamenti o forniture di dati.

Allegati malevoli: File che installano malware o ransomware.

Link malevoli: Che portano a pagine fasulle progettate per raccogliere credenziali.

- **Obiettivo:**

Rubare informazioni sensibili (es. credenziali di accesso).

Installare malware o trojan.

Avviare una compromissione della rete (es. nel caso di attacchi BEC - Business Email Compromise).

---

### 3. **Pretexting:**

- Il pretexting è una tecnica di social engineering in cui l'attaccante crea una falsa narrativa (pretesto) per ottenere informazioni sensibili o accesso a risorse protette. In pratica, l'attaccante si maschera da persona autorevole o di fiducia, come un tecnico IT, un responsabile di sicurezza o un rappresentante di una compagnia, con l'obiettivo di manipolare la vittima a fornire dettagli riservati, credenziali o accesso a sistemi aziendali.
- **Come funziona il Pretexting:**
  - **Creazione del pretesto:**

L'attaccante raccoglie informazioni preliminari sulla vittima (ad esempio il suo ruolo, colleghi o la sua attività professionale) tramite fonti pubbliche come social media, siti aziendali o comunicati stampa.

Utilizza queste informazioni per costruire una falsa identità credibile. Per esempio, si può presentare come un tecnico IT che ha bisogno di accesso alle credenziali per risolvere un "problema urgente".
  - **Contatto con la vittima:**

L'attaccante si presenta come una persona conosciuta, invia email o fa telefonate per indurre la vittima a credere che una determinata azione sia necessaria per il suo ruolo (ad esempio, una richiesta urgente di modifica delle credenziali).

Il pretesto può variare: l'attaccante potrebbe fingere di essere un tecnico che esegue una manutenzione, un audit che verifica i permessi di accesso, o un operatore che fornisce supporto in caso di emergenza.
  - **Ottenimento dell'informazione:**

Una volta che la vittima è convinta della legittimità della richiesta, fornisce le informazioni richieste o consente l'accesso a sistemi o dati sensibili. Questi potrebbero includere:

    - Credenziali di accesso.
    - Dettagli finanziari.
    - Dati aziendali confidenziali.
    - Accesso fisico a determinate aree.

---

### 4. **Baiting:**

- Il baiting è una tecnica di social engineering che sfrutta l'attrazione per qualcosa di desiderabile (un "esca") per indurre la vittima a compiere un'azione che comprometta la sua sicurezza. Gli attacchi di baiting sono simili a un "esca" in cui l'attaccante offre qualcosa di allettante, ma in realtà l'obiettivo è quello di sfruttare la vittima per ottenere accesso a risorse sensibili o installare malware.
  - **Come funziona il Baiting:**
    - **Creazione della tentazione:**

L'attaccante presenta un'offerta allettante che potrebbe essere un prodotto, servizio, o persino un oggetto fisico lasciato incustodito. Alcuni esempi comuni:

Chiavette USB infette: L'attaccante può lasciare una chiavetta USB in un luogo pubblico, come una zona comune dell'ufficio o nel parcheggio di un'azienda. Quando la vittima collega la chiavetta al proprio dispositivo, il malware si installa automaticamente.

Download di software gratuito: Un sito web o un pop-up pubblicitario che promette software gratuito (ad esempio antivirus o giochi), ma che in realtà contiene malware.
    - **Tentazione o offerta ingannevole:**

Gli attaccanti spesso usano messaggi accattivanti, come "gratis", "offerta limitata", "risparmia subito", per spingere le vittime a cliccare o interagire con il contenuto. La promessa di un vantaggio immediato, come un premio o un software gratuito, rende più facile abbassare la guardia.
    - **Compromissione e exploit:**

Una volta che la vittima interagisce con l'esca (ad esempio, aprendo un allegato infetto o collegando una chiavetta USB), il malware o il trojan si attiva, con conseguente:

Installazione di virus, ransomware o spyware sul dispositivo.

Furto di informazioni sensibili come credenziali di accesso, dati bancari, o altre informazioni personali.

Creazione di backdoor per accessi futuri non autorizzati.
- 

## 5. Tailgating/Piggybacking:

- Il tailgating (o piggybacking) è una tecnica di attacco fisico che sfrutta la fiducia e l'azione di un dipendente per ottenere accesso non autorizzato a zone sicure, come edifici aziendali o server rooms. Questo tipo di attacco non richiede competenze tecniche avanzate, ma si basa su tattiche psicologiche che inducono una persona a facilitare l'ingresso di un attaccante.
- **Come funziona il Tailgating/Piggybacking**
  - **L'attacco inizia con la raccolta di informazioni:**

Gli attaccanti osservano i movimenti e le routine dei dipendenti, cercando di cogliere momenti di disattenzione o comportamenti di fiducia (ad esempio, una porta lasciata aperta o un collega che passa senza controllare il badge).
  - **Intrusione fisica:**

L'attaccante si avvicina a una zona protetta e si infila nel flusso di persone autorizzate. Approfitta della distrazione della vittima o della cortesia (come tenere la porta aperta per un

collega) per entrare senza farsi notare.

Spesso, il termine "piggybacking" si riferisce all'atto di un attaccante che segue qualcuno senza il permesso, mentre "tailgating" può descrivere anche l'intrusione in spazi più stretti dove l'attaccante può agganciarsi fisicamente dietro una persona autorizzata.

- **Accesso a aree protette:**

Una volta all'interno, l'attaccante può accedere a computer, dispositivi sensibili o altre informazioni riservate senza essere rilevato, sfruttando l'accesso fisico alle risorse aziendali.

---

## 6. Quid Pro Quo

- Il quid pro quo (latino per "qualcosa in cambio di qualcos'altro") è una tecnica di social engineering in cui un attaccante offre un beneficio o un servizio in cambio di informazioni sensibili, credenziali o accesso non autorizzato. È una delle forme più subdole di manipolazione, in quanto si basa su una relazione di "scambio" che sembra vantaggiosa per entrambe le parti.

Questa tecnica è simile a baiting (attacco con esca), ma l'offerta fatta dall'attaccante si concentra su un beneficio diretto e immediato per la vittima, come la risoluzione di un problema tecnico, supporto software gratuito, o altro.

- **Come funziona il Quid Pro Quo:**

- **Inizio della manipolazione:**

L'attaccante entra in contatto con la vittima e propone un "servizio" che sembra utile. Ad esempio, può proporsi come tecnico di supporto o consulente IT.

- **Offerta di aiuto:**

L'attaccante offre di risolvere un problema, come un malfunzionamento del computer, il recupero di una password o l'installazione di un software.

L'offerta sembra vantaggiosa e potrebbe sembrare legittima perché viene presentata in modo professionale.

- **Richiesta in cambio:**

In cambio, l'attaccante chiede informazioni sensibili, come credenziali di accesso, dati bancari, o l'autorizzazione a installare software dannoso (malware, spyware, ecc.).

Talvolta, l'attaccante potrebbe anche chiedere l'accesso remoto al dispositivo della vittima, promettendo supporto tecnico.

- **Conclusione dell'attacco:**

Una volta ottenuto l'accesso o le informazioni richieste, l'attaccante può compromettere i sistemi, rubare dati sensibili, o persino eseguire attacchi successivi (come ransomware o furto di identità).

---

## 7. Dumpster Diving

- Il Dumpster Diving è una tecnica di attacco che si basa sulla ricerca di informazioni riservate o sensibili negli scarti fisici di un'organizzazione, come i rifiuti, le stampanti o le vecchie cartucce

di hard disk. Sebbene sembri un metodo primitivo, questo tipo di attacco può rivelarsi estremamente efficace, in quanto molte persone non considerano i rifiuti come una fonte di rischio per la sicurezza.

- **Come funziona il Dumpster Diving:**

- **Raccolta di rifiuti fisici:**

- Gli attaccanti ispezionano i cassonetti aziendali, le aree di smaltimento dei rifiuti o anche i bidoni di carta delle scrivanie per cercare documenti, carte, dispositivi o supporti di archiviazione che contengano informazioni sensibili.

- **Obiettivi:**

- **Documenti cartacei:** Contratti, report aziendali, appunti con password o dati personali, fatture.

- **Dispositivi e supporti di archiviazione:** Hard disk, chiavette USB, dischi rigidi o vecchi computer contenenti dati non adeguatamente distrutti.

- Informazioni aziendali: Documenti legali, piani di business, strategie di marketing, dettagli su clienti o fornitori.

- **Elementi non protetti:** Cartelle archiviate con password scritte a mano o note con codici di accesso.

- Obiettivi principali:

- **Ottenere informazioni sensibili:** L'accesso a dati aziendali riservati, credenziali di accesso, numeri di carta di credito, password o altre informazioni personali.

- **Accesso a reti aziendali:** I dati rubati possono essere utilizzati per accedere a reti aziendali o a sistemi di pagamento.

- **Completamento di attacchi di social engineering:** Utilizzare informazioni ottenute per creare attacchi mirati o truffe, come il phishing.

---

## 8. Watering Hole Attack

- Il watering hole attack è una sofisticata tecnica di attacco in cui gli aggressori compromettano un sito web che è frequentemente visitato da un target specifico, come ad esempio i dipendenti di una determinata azienda. Il nome "watering hole" si ispira all'idea che gli attaccanti "siano in agguato" nei luoghi frequentati dalle loro vittime, proprio come un predatore che attende vicino a una pozza d'acqua.

- **Come funziona il Watering Hole Attack:**

- **Identificazione del target:**

- Gli attaccanti iniziano monitorando l'organizzazione o il gruppo di interesse per identificare quali siti web sono frequentemente visitati dai dipendenti. Questi possono includere siti di notizie, portali aziendali, blog di settore o altre risorse professionali.

- **Compromissione del sito:**

- Una volta identificato un sito web affidabile ma vulnerabile, l'attaccante lo compromette, inserendo codice maligno (ad esempio malware o exploit) nelle sue pagine o nei suoi script.

- **Contaminazione degli utenti:**

Quando i dipendenti della vittima visitano il sito compromesso, il codice dannoso viene eseguito automaticamente sul loro sistema, sfruttando vulnerabilità nel browser o in plugin non aggiornati. Questo può portare all'installazione di malware, trojan, spyware o ransomware.

- **Obiettivi:**

- **Rubare credenziali e informazioni sensibili:** Raccogliere dati tramite keylogger o altre forme di malware.
- **Rilevare vulnerabilità della rete:** Usare il malware per fare il reconnaissance del sistema o esplorare la rete aziendale.
- **Installare backdoor:** Consentire accessi non autorizzati in futuro.

---

## Prevenzione contro le tecniche di Social Engineering

---

Le tecniche di social engineering si concentrano sulla manipolazione delle persone piuttosto che sullo sfruttamento di vulnerabilità tecnologiche. Gli attaccanti utilizzano tecniche psicologiche per ingannare le vittime e ottenere informazioni sensibili o l'accesso a sistemi aziendali. La prevenzione contro queste tecniche richiede un approccio combinato che coinvolga tecnologia, formazione e consapevolezza comportamentale. Di seguito, un approfondimento su come prevenire le varie tecniche di social engineering.

### 1. Phishing:

- **Educazione e formazione del personale:** Formare i dipendenti a riconoscere segnali di phishing, come indirizzi email strani, errori grammaticali, link sospetti o richieste di informazioni urgenti.
- **Autenticazione a due fattori (2FA):** Implementare la 2FA su tutti i sistemi aziendali per ridurre i danni se le credenziali vengono compromesse.
- **Filtri di posta elettronica:** Utilizzare soluzioni di sicurezza avanzate per filtrare automaticamente le email di phishing. Strumenti come Microsoft Defender, Proofpoint o Barracuda possono bloccare le email sospette.
- **Verifica dei link:** Prima di cliccare su un link, posizionare il cursore sopra di esso per verificare l'URL. Evitare di cliccare su link sospetti.

### 2. Spear Phishing:

- **Verifica delle richieste sensibili:** In caso di richieste di azioni urgenti, come il trasferimento di denaro o la divulgazione di dati sensibili, verificare l'autenticità della richiesta con un canale di comunicazione separato (ad esempio, una telefonata).
- **Minimizzazione delle informazioni online:** Limitare la quantità di informazioni personali disponibili su social media e siti aziendali che potrebbero essere utilizzate per personalizzare gli



attacchi.

- **Educazione avanzata:** Formare i dipendenti su come identificare segnali di spear phishing, come la familiarità eccessiva nelle email o richieste inusuali da colleghi o superiori.

### 3. **Pretexting:**

- **Verifica dell'identità:** Mai fornire informazioni sensibili a chi non si è verificato adeguatamente. Utilizzare sempre un canale separato per confermare l'identità di chi richiede dati.
- **Politiche aziendali di gestione delle informazioni:** Stabilire chiare linee guida su chi ha accesso a cosa, e su come le informazioni devono essere condivise internamente.
- **Consapevolezza e formazione:** Educare i dipendenti a non rivelare informazioni aziendali o personali a chiunque si presenti come un estraneo, anche se la richiesta sembra legittima.

### 4. **Baiting:**

- **Politiche di sicurezza dei dispositivi:** Non utilizzare dispositivi USB sconosciuti e fare attenzione a qualsiasi dispositivo lasciato incustodito.
- **Protezione antivirus e anti-malware:** Utilizzare software antivirus aggiornato che possa rilevare e bloccare malware da dispositivi esterni.
- **Formazione dei dipendenti:** Educare i dipendenti sull'uso sicuro dei dispositivi e sull'importanza di non collegare dispositivi esterni non verificati ai sistemi aziendali.

### 5. **Tailgating/Piggybacking>**

- **Controllo degli accessi fisici:** Utilizzare sistemi di badge elettronici, accesso biometrico o codici di accesso per garantire che solo il personale autorizzato possa entrare in aree protette.
- **Politiche di sicurezza fisica:** I dipendenti devono essere addestrati a non permettere l'ingresso a persone sconosciute e a segnalare chiunque tenti di entrare senza autorizzazione.
- **Sensibilizzazione:** Promuovere la cultura della sicurezza tra i dipendenti, facendo loro capire l'importanza di non "tenere aperta" la porta per estranei, anche se sembra innocuo.

### 6. **Quid Pro Quo:**

- **Verifica delle offerte:** Non accettare mai offerte che sembrano troppo belle per essere vere. In caso di richieste sospette, verificare sempre l'identità della persona che fa l'offerta.
- **Gestione delle richieste interne:** Stabilire politiche interne che non richiedano mai di fornire dati sensibili in cambio di servizi o vantaggi, senza una chiara giustificazione.
- **Formazione sulle truffe comuni:** Educare i dipendenti a riconoscere questo tipo di attacco e a rifiutare qualsiasi offerta che sembri sospetta o non motivata.

### 7. **Dumpster Diving:**

- **Distruzione sicura dei documenti:** Una delle migliori difese è distruggere i documenti sensibili prima di gettarli via. Utilizzare trituratori di carta sicuri per distruggere i dati aziendali, comprese

le informazioni personali di dipendenti e clienti.

- **Politiche aziendali sui dati sensibili:** Implementare procedure chiare per il trattamento dei documenti sensibili. Questi devono essere smaltiti in modo sicuro, e non solo gettati via in contenitori per i rifiuti. Le aziende dovrebbero mantenere un inventario di come vengono distrutti i dati fisici e digitali.
- **Educazione dei dipendenti:** I dipendenti dovrebbero essere educati sulla protezione delle informazioni aziendali e personali. Devono essere consapevoli che i documenti aziendali non devono essere lasciati incustoditi, nemmeno per un breve periodo, e che le informazioni sensibili devono essere trattate con attenzione, anche quando vengono eliminati.
- **Controllo dei bidoni dei rifiuti:** Eseguire controlli regolari per accertarsi che i rifiuti aziendali non contengano documenti non distrutti correttamente. È utile stabilire una politica che impone la supervisione o la registrazione quando si gestiscono i rifiuti aziendali.

## 8. **Watering Hole Attack:**

- **Protezione dei siti web aziendali:** Le organizzazioni devono essere proattive nella protezione dei loro siti web aziendali contro le vulnerabilità. Questo include l'uso di firewall applicativi e di misure di sicurezza avanzate come la scansione continua di vulnerabilità. Il controllo regolare della sicurezza delle applicazioni web è fondamentale.
- **Monitoraggio dei siti web frequentati dai dipendenti:** Le aziende dovrebbero monitorare e restringere l'accesso a siti web che potrebbero essere rischiosi. Implementare un sistema di controllo della navigazione (web filtering) che blocchi l'accesso a siti web sospetti o non sicuri.
- **Aggiornamenti e patching continuo:** Mantenere tutti i sistemi, sia interni che quelli utilizzati per la navigazione web, aggiornati con le ultime patch di sicurezza per evitare che gli attaccanti sfruttino vulnerabilità note nei siti web legittimi.
- **Formazione sui rischi dei siti web compromessi:** Educare i dipendenti sui rischi dei siti web e su come evitare di visitare siti sconosciuti o non sicuri. I dipendenti devono essere informati su come riconoscere possibili tentativi di attacco.
- **Uso di software di sicurezza avanzato:** Utilizzare soluzioni di antivirus e di protezione da malware che possano rilevare e bloccare minacce provenienti da siti web compromessi.
- **Isolamento delle reti interne:** Utilizzare un sistema di rete segmentato, in modo che, se un dispositivo viene compromesso da un sito web dannoso, l'accesso ai sistemi aziendali più sensibili venga limitato e contenuto.

---

## **Conclusione**

Le tecniche di *social engineering* rappresentano una delle principali minacce per la sicurezza informatica, poiché si basano sulla manipolazione delle persone anziché su vulnerabilità tecnologiche. Gli attaccanti sfruttano la psicologia umana, la fiducia e l'ignoranza per ottenere informazioni sensibili, compromettere sistemi aziendali e causare danni. Tuttavia, con l'adozione di strategie di prevenzione adeguate, è possibile ridurre significativamente il rischio di cadere vittima di questi attacchi.

La formazione continua dei dipendenti è la chiave per rafforzare la consapevolezza del rischio e sviluppare una cultura della sicurezza che possa difendere l'azienda da attacchi di phishing, spear phishing, pretexting, e altre tecniche comuni. Implementare tecnologie di sicurezza come l'autenticazione a due fattori (2FA), l'uso di antivirus avanzati, e il monitoraggio attivo delle reti può ulteriormente proteggere le risorse aziendali. Inoltre, politiche rigorose di gestione dei dati sensibili, sia fisici che digitali, possono ridurre il rischio di attacchi come il *dumpster diving* e gli *watering hole attacks*.

Infine, la protezione contro gli attacchi di social engineering richiede un approccio integrato che coinvolga non solo la tecnologia, ma anche la cultura aziendale e le pratiche quotidiane. Solo un impegno collettivo nella prevenzione, nella consapevolezza e nella vigilanza costante può garantire che le organizzazioni siano in grado di difendersi efficacemente da queste minacce sempre più sofisticate.