

CYBERSICUREZZA / INGEGNERIA SOCIALE

PHISHING

Dalle origini alle minacce contemporanee



Evoluzione delle tecniche, misure di contenimento e profili giuridici

Vincenzo Calabrò

Edizione 2026

Abstract

Il phishing accompagna la diffusione dei servizi digitali da oltre trent'anni. Le prime campagne miravano soprattutto alla sottrazione di credenziali e dati finanziari; quelle attuali colpiscono identità cloud, sessioni autenticate, procedure di pagamento e relazioni professionali già consolidate. Il saggio ripercorre questa evoluzione, descrive le tecniche oggi più ricorrenti e valuta le difese disponibili sul piano tecnico e organizzativo. L'ultima parte esamina le conseguenze giuridiche dell'incidente, con riferimento alla protezione dei dati personali, alla disciplina NIS2 e alle fattispecie penali che possono venire in rilievo. La ricostruzione si fonda su fonti normative, documentazione istituzionale e rapporti tecnici disponibili al 2026.

Indice

01	Origini ed evoluzione storica
02	Anatomia dell'attacco
03	Forme contemporanee
04	Il fattore umano e organizzativo.....
05	Misure di prevenzione e contenimento
06	Gestione dell'incidente.....
07	Profili giuridici.....
08	Conclusioni

01 Origini ed evoluzione storica

Il phishing non nasce con l'home banking e non coincide con una particolare tecnologia. È, prima di tutto, un modo di sfruttare la fiducia nei sistemi di comunicazione e nei soggetti che li utilizzano. Le tecniche cambiano insieme ai servizi digitali; resta stabile la necessità di rendere credibile una richiesta che non dovrebbe esserlo.

1.1 Dall'abuso delle comunità online alla frode organizzata

Caso di studio 1.1 - Dai sistemi chiusi alle prime frodi online

Anni Ottanta e Novanta

Prima che il phishing assumesse un nome stabile, tecniche fondate sulla falsa identità e sulla richiesta diretta di informazioni erano già state descritte negli ambienti informatici. Una dimostrazione condotta nel 1984 sul sistema EIES del New Jersey Institute of Technology e una presentazione del 1987 all'International HP Users Group anticipavano elementi poi divenuti tipici: costruzione di un'identità credibile, richiesta apparentemente legittima e acquisizione di informazioni riservate [17]. **Indicazione ricavabile dal caso:** il phishing non dipende dalla posta elettronica. Il tratto costante è la manipolazione del rapporto di fiducia tra utente e sistema.

Le prime pratiche riconducibili al phishing precedono la diffusione dell'home banking. Negli anni Novanta, nei servizi online a larga diffusione, soggetti malevoli impersonavano operatori o amministratori per convincere gli utenti a rivelare credenziali e dati di fatturazione. La novità non consisteva nell'inganno in sé, già noto nelle frodi tradizionali, ma nella possibilità di replicarlo a distanza, a costi ridotti e nei confronti di un numero elevato di destinatari.

Con l'espansione del web commerciale, l'imitazione delle interfacce divenne parte integrante dell'attacco. Il messaggio fraudolento indirizzava la vittima verso una pagina costruita per riprodurre l'aspetto di un servizio legittimo. L'uso di domini somiglienti, collegamenti mascherati e moduli di autenticazione contraffatti permetteva di sottrarre credenziali bancarie, numeri di carta e informazioni personali. La posta elettronica, progettata in un ambiente fondato sulla fiducia reciproca tra sistemi, offriva agli attaccanti un canale particolarmente favorevole.

1.2 La fase bancaria e la standardizzazione del modello

Caso di studio 1 - AOL e la nascita del phishing

Metà degli anni Novanta

Negli ambienti di America Online, gli aggressori si presentavano come addetti del servizio e chiedevano agli utenti di verificare l'account o confermare i dati di fatturazione. Strumenti come AOHell resero più semplice automatizzare l'impersonificazione e il furto delle credenziali. Il bersaglio iniziale non era ancora l'home banking: erano l'accesso al servizio, le password e i dati necessari ad aprire o mantenere gli account [12]. **Indicazione ricavabile dal caso:** il phishing nasce come abuso della fiducia riposta nell'amministratore del servizio. Cambiano le piattaforme, ma il pretesto della verifica dell'account resta tuttora ricorrente.

Tra la fine degli anni Novanta e i primi anni Duemila il phishing assunse una configurazione riconoscibile: un messaggio apparentemente proveniente da una banca, da un servizio di pagamento o da una piattaforma commerciale segnalava un problema urgente e sollecitava una verifica. La sequenza era semplice e ripetibile: impersonificazione del mittente, costruzione di un pretesto, riduzione del tempo disponibile per decidere, trasferimento verso un ambiente controllato dall'attaccante e raccolta delle informazioni.

Nel 2003 nacque l'Anti-Phishing Working Group. La raccolta coordinata delle segnalazioni offrì una base più solida per seguire l'andamento delle campagne e mise in relazione fornitori tecnologici, operatori finanziari, registri di dominio e gruppi di risposta agli incidenti [1].

1.3 Dal messaggio di massa alla compromissione del processo

Caso di studio 1.3 - La compromissione di un fornitore come punto di ingresso

Target, 2013

Nel 2013 gli attaccanti utilizzarono credenziali sottratte a un fornitore esterno per accedere alla rete di Target. Da quel punto si spostarono verso i sistemi di vendita e distribuirono malware destinato alla raccolta dei dati delle carte di pagamento. L'incidente interessò circa 40 milioni di carte e mostrò come una credenziale appartenente a una relazione commerciale potesse diventare il punto di ingresso verso sistemi molto più sensibili [18]. **Indicazione ricavabile dal caso:** il bersaglio effettivo può essere raggiunto attraverso un soggetto terzo. La gestione del rischio deve comprendere accessi dei fornitori, segmentazione, minimo privilegio e risposta agli allarmi.

Nella prima fase le campagne puntavano soprattutto sulla quantità. La personalizzazione era limitata e gli errori linguistici costituivano spesso un indizio utile. La disponibilità di dati pubblici, violazioni pregresse, social network e servizi di profilazione ha successivamente reso economica la selezione del bersaglio. Il phishing contemporaneo non si limita a imitare un marchio: ricostruisce relazioni, ruoli, scadenze e procedure.

L'obiettivo si è esteso dalla password al controllo dell'identità digitale. Una compromissione può consentire di leggere la corrispondenza, osservare le abitudini dell'organizzazione, modificare regole di inoltro, registrare nuovi metodi di autenticazione, autorizzare applicazioni, sottrarre documenti o inserirsi in trattative economiche già in corso. La compromissione, dunque, non resta confinata al singolo account. Può alterare l'affidabilità di un procedimento amministrativo, di una trattativa o di un flusso di pagamento.

Dato di contesto

Nel primo trimestre 2025 l'APWG ha rilevato 1.003.924 attacchi di phishing. Nello stesso periodo sono cresciuti gli attacchi mediante codice QR e le frodi BEC finalizzate ai bonifici [2]. Nel secondo trimestre 2026 l'organizzazione ha registrato un ulteriore aumento, con crescita dello smishing e degli attacchi BEC [1].

02 Anatomia dell'attacco

2.1 Ricognizione, pretesto e canale

Caso di studio 2.1 - Ricognizione e pretesto nel caso Twitter

Luglio 2020

Gli autori dell'attacco contro Twitter individuarono dipendenti e ruoli utili, quindi ricorsero al phone spear phishing impersonando il supporto interno. Le prime credenziali ottenute servirono anche a comprendere processi e strumenti dell'organizzazione e a raggiungere personale dotato di accessi più elevati. Furono coinvolti 130 account e alcuni profili compromessi vennero utilizzati per una frode in bitcoin [19]. **Indicazione ricavabile dal caso:** la ricognizione non serve soltanto a scegliere la vittima. Può proseguire dopo il primo accesso e fornire le informazioni necessarie per colpire ruoli privilegiati.

Gli episodi osservati presentano spesso una sequenza riconoscibile. La ricognizione individua il bersaglio e raccoglie informazioni sufficienti a costruire un pretesto. Seguono la

scelta del canale, la preparazione dell'identità apparente e la definizione dell'azione richiesta. L'attaccante non deve necessariamente convincere la vittima di ogni dettaglio; gli basta rendere plausibile il gesto decisivo: selezionare un collegamento, aprire un allegato, approvare una richiesta o modificare un pagamento.

I pretesti più convincenti fanno leva sull'autorità del mittente, sulla pressione del tempo e sulla familiarità della richiesta. Un avviso tecnico, una richiesta del dirigente, una fattura, una condivisione documentale o una comunicazione istituzionale funzionano perché si inseriscono in attività ordinarie. Il rischio cresce quando la procedura organizzativa consente eccezioni informali, quando le responsabilità non sono chiare o quando la verifica viene affidata allo stesso canale dal quale proviene la richiesta.

2.2 Acquisizione delle credenziali e della sessione

Caso di studio 2.2 - Consent phishing e autorizzazioni OAuth

Campagna resa pubblica nel gennaio 2023

Microsoft ha ricostruito una campagna nella quale gli aggressori creano applicazioni OAuth associate a falsi profili di partner verificati. Gli utenti venivano indotti ad approvare le autorizzazioni richieste dall'applicazione; dopo il consenso, gli aggressori utilizzavano l'accesso ottenuto per esfiltrare la posta elettronica. La tecnica non richiedeva necessariamente la sottrazione della password [20]. **Indicazione ricavabile dal caso:** il controllo dell'identità deve includere le applicazioni autorizzate. Reimpostare la password non revoca automaticamente un consenso OAuth già concesso.

Le pagine contraffatte restano diffuse, ma i meccanismi si sono evoluti. Negli attacchi adversary-in-the-middle, un'infrastruttura fraudolenta si interpone tra l'utente e il servizio legittimo e può acquisire in tempo reale credenziali e cookie o token di sessione. In altri casi l'utente viene indotto a concedere autorizzazioni OAuth a un'applicazione malevola. L'accesso può quindi essere ottenuto senza disporre stabilmente della password oppure dopo che la vittima ha completato una forma di autenticazione multifattore suscettibile di phishing.

Il furto della sessione obbliga a guardare oltre il momento dell'accesso. Durata e revoca delle sessioni, registrazione dei dispositivi, autorizzazioni applicative e anomalie di autenticazione diventano parte dello stesso problema. La protezione dell'identità non si esaurisce, quindi, nella verifica iniziale delle credenziali.

2.3 Persistenza, monetizzazione e danno

Caso di studio 2 - La compromissione RSA SecurID

Marzo 2011

Un'e-mail di spear phishing, inviata a piccoli gruppi di dipendenti RSA e recuperata dalla cartella della posta indesiderata, conteneva un file Excel denominato "2011 Recruitment Plan". L'allegato sfruttava una vulnerabilità zero-day di Adobe Flash e installava una backdoor. Gli attaccanti proseguirono con escalation dei privilegi, movimento laterale ed esfiltrazione di informazioni relative a SecurID [13]. **Indicazione ricavabile dal caso:** il messaggio iniziale può apparire marginale rispetto al danno finale. Il contenimento deve considerare l'intera catena, dall'endpoint alla compromissione di sistemi e dipendenze critiche.

Una volta ottenuto l'accesso, l'attaccante può mantenere la presenza mediante regole di posta, deleghe, applicazioni autorizzate o nuovi metodi di recupero. La monetizzazione può avvenire attraverso trasferimenti di denaro, rivendita delle credenziali, estorsione, esfiltrazione di dati o uso dell'account per colpire altri soggetti. Una casella compromessa è particolarmente utile perché conserva il contesto necessario a costruire messaggi credibili.

03 Forme contemporanee

3.1 Spear phishing, whaling e BEC

Caso di studio 1 - BEC e false istruzioni di pagamento

2013-2015

Secondo il Dipartimento di Giustizia statunitense, Evaldas Rimasauskas organizzò una frode che indusse due società Internet statunitensi a trasferire complessivamente oltre 120 milioni di dollari. Lo schema riproduceva l'identità di un fornitore asiatico realmente coinvolto in rapporti commerciali con le vittime e accompagnava le richieste di pagamento con e-mail e documentazione contraffatta [14]. **Indicazione ricavabile dal caso:** la familiarità del fornitore, la plausibilità della fattura e la correttezza formale del messaggio non sostituiscono la verifica indipendente delle coordinate di pagamento.

Lo spear phishing seleziona un destinatario o un gruppo ristretto e adatta il contenuto al ruolo svolto. Quando il bersaglio è un dirigente o un soggetto dotato di poteri autorizzativi si parla spesso di whaling. Nelle frodi Business Email Compromise l'attaccante impersona o

compromette una casella reale per interferire con pagamenti, fatture, contratti o informazioni riservate. La variante Vendor Email Compromise sfrutta invece la fiducia riposta in un fornitore.

Rispetto alle campagne indiscriminate, cambia soprattutto il grado di aderenza al contesto reale. Il messaggio può provenire da un account autentico, riferirsi a una pratica esistente e rispettare le convenzioni linguistiche dell'organizzazione. La verifica puramente formale del mittente non è sufficiente; serve un controllo sul processo e sull'anomalia della richiesta.

3.2 Smishing, vishing, callback phishing e quishing

Caso di studio 2 - Callback phishing a tema autorità

Italia, aprile 2025

CSIRT Italia ha documentato una campagna che utilizzava il nome e il logo della Polizia di Stato. Il messaggio richiama un presunto procedimento penale, allegava un PDF con una firma artefatta e sollecitava una risposta urgente. L'obiettivo era instaurare un contatto diretto nel quale l'attaccante potesse controllare la narrazione e raccogliere informazioni [15]. **Indicazione ricavabile dal caso:** autorità apparente, gravità dell'accusa e urgenza sono elementi del pretesto. La verifica deve avvenire tramite recapiti istituzionali già noti, senza rispondere al messaggio ricevuto.

Il phishing è ormai multicanale. Lo smishing utilizza SMS e messaggistica istantanea; il vishing ricorre alla voce; il callback phishing induce il destinatario a chiamare un numero controllato dall'attaccante. Il quishing incorpora un codice QR in un messaggio o in un documento, spostando spesso la navigazione su un dispositivo mobile meno integrato con i controlli dell'organizzazione.

L'uso coordinato di più canali rende il pretesto più plausibile. Un'e-mail può anticipare una telefonata, un SMS può rimandare a un portale e una voce sintetica può rafforzare l'impersonificazione. La contromisura principale non consiste nell'indovinare se la voce o il documento siano falsi, ma nel ricondurre la richiesta a una procedura verificabile e a recapiti già noti.

3.3 Intelligenza artificiale e contenuti sintetici

Caso di studio 3.3 - Videoconferenza sintetica e frode finanziaria

Hong Kong, 2024

Secondo la ricostruzione resa pubblica dalla polizia di Hong Kong, un dipendente dell'area finanziaria partecipò a una videoconferenza nella quale il direttore finanziario e altri colleghi apparivano autentici, ma erano riproduzioni sintetiche. Il dipendente eseguì trasferimenti per complessivi 200 milioni di dollari di Hong Kong, circa 25 milioni di dollari statunitensi [21]. **Indicazione ricavabile dal caso:** la riconoscibilità di un volto o di una voce non costituisce più una verifica sufficiente. Le operazioni ad alto valore richiedono autorizzazioni registrate e un controllo indipendente dal canale nel quale nasce la richiesta.

I sistemi generativi riducono il costo della personalizzazione linguistica e consentono di produrre messaggi coerenti con lingua, registro e settore del destinatario. L'impiego di contenuti sintetici rende meno affidabili indicatori tradizionali quali errori ortografici o formulazioni innaturali. La stessa tecnologia può essere impiegata per creare immagini, audio e video destinati a sostenere un pretesto.

Il rapporto ENISA Threat Landscape 2025 prende in esame 4.875 incidenti osservati tra il 1° luglio 2024 e il 30 giugno 2025. Il phishing vi figura tra i principali vettori di accesso iniziale, in un contesto nel quale l'automazione rende più agevole produrre e adattare contenuti di ingegneria sociale [3]. Il phishing non può più essere identificato con il solo messaggio grossolano, riconoscibile dagli errori di lingua.

3.4 Ecosistemi cloud e piattaforme collaborative

Caso di studio 3 - AiTM e abuso di SharePoint

Campagna resa pubblica nel gennaio 2026

Microsoft ha descritto una campagna multistadio rivolta a organizzazioni del settore energetico. I messaggi, provenienti da identità attendibili già compromesse, utilizzavano condivisioni SharePoint come esca. Dopo il furto della sessione, gli attaccanti creavano regole nella casella di posta e impiegavano gli account compromessi per ulteriori attività di phishing e BEC [16]. **Indicazione ricavabile dal caso:** il cambio della password non è sufficiente quando sono stati sottratti cookie di sessione o sono state create forme di persistenza. Occorre revocare le sessioni, verificare regole di posta e autorizzazioni e ricostruire gli accessi successivi.

Le campagne contemporanee imitano portali di accesso, notifiche di condivisione, inviti a riunioni e avvisi relativi allo spazio disponibile. Le piattaforme collaborative offrono all'attaccante un ambiente familiare e permettono di sfruttare servizi legittimi per ospitare contenuti o reindirizzamenti. La compromissione di un'identità cloud può propagarsi rapidamente attraverso rubriche, documenti condivisi e relazioni fra tenant.

Il Verizon Data Breach Investigations Report 2025 considera 22.052 incidenti, dei quali 12.195 qualificati come violazioni confermate, relativi a organizzazioni di 139 Paesi. Nel campione restano rilevanti il social engineering, l'abuso delle credenziali e il coinvolgimento di soggetti terzi [4].

04 Il fattore umano e organizzativo

4.1 Oltre la nozione di errore umano

Caso di studio 4.1 - Il service desk come controllo organizzativo

MGM Resorts, settembre 2023

L'attacco contro MGM Resorts fu ricondotto a una campagna di ingegneria sociale nella quale informazioni pubbliche sui dipendenti furono utilizzate per rendere credibile una chiamata al service desk. L'accesso iniziale contribuì a una compromissione con estese interruzioni operative, che interessarono prenotazioni, chiavi digitali e altri servizi. L'episodio mise in evidenza il peso delle procedure di verifica adottate dall'assistenza tecnica [22]. **Indicazione ricavabile dal caso:** l'operatore del service desk non è un elemento esterno alla sicurezza dell'identità. Le procedure di recupero e reset devono prevedere verifiche indipendenti, escalation e tracciabilità.

Ricondurre l'incidente alla sola distrazione dell'utente nasconde una parte essenziale del problema. Le persone operano in sistemi caratterizzati da carichi di lavoro, interruzioni, asimmetrie informative e pressioni temporali. L'attaccante progetta il messaggio proprio per sfruttare tali condizioni. Se un pagamento può essere modificato da una singola e-mail, il problema riguarda il processo prima ancora della condotta individuale.

Una risposta esclusivamente punitiva può aggravare le conseguenze dell'incidente, perché induce a ritardare la segnalazione. La rapidità con cui l'organizzazione viene informata può determinare la possibilità di revocare una sessione, bloccare un pagamento o impedire la diffusione interna. L'utente deve quindi essere considerato un sensore del sistema, non l'ultimo anello debole.

4.2 Formazione, simulazioni e metriche

La formazione efficace è periodica, contestualizzata e differenziata per ruolo. Amministratori, personale finanziario, segreterie, dirigenti e addetti al protocollo sono esposti a pretesti diversi. Le simulazioni possono essere utili se autorizzate, proporzionate e orientate all'apprendimento; perdono valore quando si riducono alla misurazione del tasso di clic o alla ricerca del colpevole.

Le metriche dovrebbero includere il tempo medio di segnalazione, la capacità di riconoscere richieste anomale, la copertura della formazione, l'adozione di autenticazione resistente al phishing e la velocità di revoca delle sessioni. Un'organizzazione matura non presume di

poter eliminare ogni errore; verifica, piuttosto, quanto rapidamente riesca a riconoscerlo e a contenerne gli effetti.

05 Misure di prevenzione e contenimento

5.1 Controlli sull'identità

L'autenticazione multifattore riduce il rischio associato alla sola password, ma le modalità non offrono lo stesso livello di protezione. SMS, codici temporanei e notifiche push possono essere intercettati, inoltrati o approvati sotto pressione. CISA indica nell'autenticazione resistente al phishing la soluzione di riferimento e raccomanda metodi basati su FIDO/WebAuthn o su infrastrutture a chiave pubblica. Il number matching può ridurre il rischio di MFA fatigue, ma non offre una protezione equivalente [5].

- Adottare passkey, chiavi FIDO2 o certificati per amministratori, dirigenti e funzioni ad alto rischio.
- Applicare accesso condizionale, valutazione del dispositivo e principio del minimo privilegio.
- Ridurre la durata delle sessioni sensibili e assicurare procedure rapide di revoca.
- Governare applicazioni OAuth, deleghe, metodi di recupero e account di emergenza.
- Proteggere il ciclo di vita dell'identità, dall'attivazione alla dismissione.

5.2 Sicurezza della posta elettronica

SPF permette al titolare di un dominio di indicare i sistemi autorizzati a inviare posta per suo conto; DKIM applica una firma crittografica a specifiche parti del messaggio; DMARC verifica l'allineamento fra i domini, combina gli esiti dei controlli e consente di dichiarare una politica di trattamento. Le linee guida ACN pubblicate nell'aprile 2026 dedicano a questi protocolli un quadro operativo finalizzato a ridurre spoofing, phishing e manomissione [6].

SPF, DKIM e DMARC coprono soltanto una parte del problema dell'impersonificazione. Non impediscono l'uso di domini simili, account legittimi compromessi o servizi leciti impiegati in modo abusivo. Devono essere integrati con filtraggio reputazionale, analisi degli allegati, protezione dei collegamenti, monitoraggio dei domini, configurazione sicura dei client e procedure di segnalazione accessibili.

5.3 Controlli di processo

Una richiesta con effetti economici o amministrativi non dovrebbe essere eseguita sulla base di un solo messaggio. La variazione di un IBAN, l'invio di dati riservati, la creazione di

un'utenza privilegiata e l'approvazione di un pagamento richiedono una verifica fuori banda, effettuata attraverso un recapito già noto o un sistema indipendente.

- Separazione dei compiti e doppia autorizzazione per operazioni sensibili.
- Canali verificati per variazioni contrattuali e coordinate di pagamento.
- Registrazione e tracciabilità delle eccezioni procedurali.
- Classificazione delle informazioni e limiti alla condivisione esterna.
- Procedure specifiche per PEC, posta ordinaria, piattaforme cloud e applicativi istituzionali.

5.4 Indicazioni per l'utente

Regola operativa

Non valutare soltanto l'aspetto del messaggio. Verificare se la richiesta è attesa, coerente con il ruolo del mittente e conforme alla procedura. In presenza di urgenza, segretezza, variazioni di pagamento, richieste di credenziali o approvazioni MFA, interrompere il flusso e verificare attraverso un canale indipendente.

06 Gestione dell'incidente

6.1 Segnalazione e triage

La segnalazione deve conservare il messaggio originale, le intestazioni, gli allegati, gli URL, l'orario e il dispositivo utilizzato. L'inoltro informale può alterare elementi utili o ampliare l'esposizione; è preferibile una funzione integrata nel client o un canale dedicato. Il triage deve stabilire se vi sia stata interazione, inserimento di credenziali, approvazione MFA, esecuzione di codice o trasferimento di denaro.

6.2 Contenimento tecnico

- Revocare sessioni e token; reimpostare le credenziali da un dispositivo affidabile.
- Verificare regole di inoltro, deleghe, metodi MFA, dispositivi registrati e autorizzazioni OAuth.
- Isolare il dispositivo secondo la procedura di incident response se è stato eseguito un allegato.

- Bloccare domini, URL, hash e altri indicatori soltanto dopo averne verificato attendibilità, perimetro e possibili effetti sui servizi legittimi.
- Verificare compromissioni correlate, movimento laterale, accessi anomali ed esfiltrazione.

6.3 Contenimento organizzativo e finanziario

Se l'attacco coinvolge pagamenti, la banca deve essere contattata immediatamente tramite canali ufficiali; il recupero può dipendere dalla tempestività. Devono essere avvisati i soggetti interni competenti, valutata la necessità di informare controparti e preservate le evidenze. Nei contesti pubblici vanno coordinate le funzioni ICT, sicurezza, protezione dei dati, affari legali, comunicazione e vertice amministrativo.

6.4 Ripristino e apprendimento

Il semplice cambio della password non conclude il ripristino. Occorre rimuovere la persistenza, riesaminare le autorizzazioni, verificare l'integrità delle comunicazioni e ricostruire la sequenza dell'evento. La revisione post-incidente deve tradursi in modifiche misurabili a processi, configurazioni e formazione.

07 Profili giuridici

7.1 Riservatezza, dati personali e data breach

Un attacco di phishing può determinare una violazione di dati personali ai sensi dell'articolo 4, punto 12, del GDPR quando comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Il titolare documenta la violazione e, salvo che sia improbabile che essa presenti un rischio per i diritti e le libertà delle persone fisiche, la notifica all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro settantadue ore dal momento in cui ne è venuto a conoscenza, secondo l'articolo 33. Quando la violazione è suscettibile di presentare un rischio elevato, l'articolo 34 richiede, fatte salve le eccezioni previste dalla norma, la comunicazione agli interessati [7] [10].

La valutazione deve considerare la natura e la quantità dei dati, la possibilità di identificare gli interessati, le conseguenze prevedibili e le misure di protezione già operative. La compromissione di una casella non equivale automaticamente alla compromissione di ogni dato accessibile, ma non consente neppure di escluderla senza analisi.

7.2 NIS2 e responsabilità organizzativa

La direttiva (UE) 2022/2555 stabilisce, per i soggetti compresi nel proprio ambito di applicazione, misure di gestione dei rischi di cybersicurezza, obblighi di notifica degli incidenti e regole in materia di cooperazione, vigilanza ed esecuzione. Gli articoli 20 e 21 disciplinano, rispettivamente, la responsabilità degli organi di gestione e le misure di gestione del rischio; l'articolo 23 regola la notifica degli incidenti significativi. Fra le misure dell'articolo 21 figurano le pratiche di igiene informatica e la formazione in materia di cybersicurezza [8]. In Italia la direttiva è stata recepita con il decreto legislativo 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024; l'ACN è Autorità nazionale competente NIS e Punto di contatto unico [9].

Nel quadro NIS2 il phishing non costituisce una categoria autonoma di incidente. Assume rilievo quando determina, o concorre a determinare, un incidente significativo con effetti sui servizi del soggetto interessato. Nel decreto legislativo n. 138 del 2024, gli articoli 23, 24 e 25 riguardano, rispettivamente, gli organi di amministrazione e direttivi, le misure di gestione dei rischi e la notifica degli incidenti. Per gli incidenti significativi l'articolo 25 prevede una pre-notifica entro ventiquattro ore, una notifica entro settantadue ore e, di regola, una relazione finale entro un mese. Tali obblighi riguardano esclusivamente i soggetti essenziali e importanti ricompresi nel campo di applicazione della disciplina [9].

7.3 Profili penali

Le condotte possono integrare, secondo le circostanze, la truffa di cui all'articolo 640 c.p., la frode informatica di cui all'articolo 640-ter c.p., l'accesso abusivo a un sistema informatico o telematico di cui all'articolo 615-ter c.p. o la sostituzione di persona di cui all'articolo 494 c.p. Possono inoltre venire in rilievo l'articolo 615-quater c.p., relativo alla detenzione, diffusione e installazione abusiva di codici o altri mezzi idonei all'accesso, l'articolo 167 del Codice in materia di protezione dei dati personali e, nelle fasi di impiego o trasferimento dei proventi, le fattispecie previste dagli articoli 648-bis e seguenti c.p. La qualificazione dipende dalle modalità, dall'evento, dall'elemento soggettivo e dal rapporto fra le singole azioni. Non è perciò corretto ricondurre ogni campagna a una fattispecie unica, né indicare la pena applicabile prescindendo dal fatto concreto e dal testo normativo vigente [11] [23].

7.4 Conservazione delle evidenze e denuncia

La risposta deve preservare messaggi originali, intestazioni, log, file, indicatori, registrazioni delle attività e documentazione delle decisioni. La catena di custodia e la ripetibilità delle acquisizioni assumono rilievo quando i dati devono essere impiegati in sede disciplinare,

civile o penale. La segnalazione tecnica non sostituisce la denuncia o la querela, quando l'ordinamento le richieda.

08 Conclusioni

Dalle prime frodi rivolte agli utenti dei servizi online alle campagne contro le identità cloud, il meccanismo di fondo è rimasto riconoscibile: indurre il destinatario a considerare ordinaria un'azione che, fuori da quel contesto, apparirebbe rischiosa. Sono cambiati i canali, la qualità dell'impersonificazione e gli obiettivi. Alla sottrazione della password si sono affiancati il furto della sessione, l'abuso delle autorizzazioni cloud, la compromissione delle conversazioni e l'interferenza con processi economici e amministrativi.

Né una singola tecnologia né la sola prudenza individuale offrono, da sole, una protezione adeguata. Autenticazione resistente al phishing, sicurezza della posta, accesso condizionale, procedure di verifica, separazione dei compiti, formazione e capacità di risposta devono operare come un sistema. La misura più efficace è quella che impedisce a un singolo errore di trasformarsi in un incidente rilevante.

Sul piano giuridico, protezione dei dati, obblighi NIS2 e fattispecie penali intervengono in momenti diversi dello stesso evento: prevenzione, rilevazione, contenimento, documentazione e accertamento delle responsabilità. L'obiettivo realistico non è impedire la ricezione di ogni messaggio fraudolento, ma ridurre le possibilità di successo e conservare la capacità di reagire in tempi compatibili con il danno.

Riferimenti bibliografici e normativi

[1] Anti-Phishing Working Group, Phishing Activity Trends Report: 2nd Quarter 2026, settembre 2026, <https://apwg.org/trendreports>.

[2] Anti-Phishing Working Group, Phishing Activity Trends Report: 1st Quarter 2025, luglio 2025, <https://apwg.org/trendreports>.

[3] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025, versione 1.3, 22 settembre 2026, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>.

[4] Verizon, 2025 Data Breach Investigations Report, 2025, <https://www.verizon.com/business/resources/reports/dbir/>.

- [5] Cybersecurity and Infrastructure Security Agency (CISA), Implementing Phishing-Resistant MFA, ottobre 2022, <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>.
- [6] Agenzia per la cybersicurezza nazionale (ACN), Linee guida - Configurazione del servizio di posta elettronica per l'autenticazione, aprile 2026, <https://www.acn.gov.it/portale/linee-guida>.
- [7] Garante per la protezione dei dati personali, Violazioni di dati personali (data breach), consultato nel 2026, <https://www.garanteprivacy.it/data-breach>.
- [8] Parlamento europeo e Consiglio, Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity nell'Unione, in particolare artt. 20, 21 e 23, testo consolidato, EUR-Lex, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.
- [9] Decreto legislativo 4 settembre 2024, n. 138, in particolare artt. 23, 24 e 25, Gazzetta Ufficiale, Serie generale n. 230 del 1° ottobre 2024, entrata in vigore 16 ottobre 2024, <https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG>.
- [10] Parlamento europeo e Consiglio, Regolamento (UE) 2016/679 del 27 aprile 2016, in particolare artt. 4, punto 12, 33 e 34, EUR-Lex, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [11] Regio decreto 19 ottobre 1930, n. 1398, Codice penale, artt. 494, 615-ter, 615-quater, 640, 640-ter e 648-bis e seguenti, testo vigente al 2026, Normattiva, <https://www.normattiva.it/>.
- [12] Cisco, Security History: The Evolution of Phishing, 6 febbraio 2023, <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m02/security-history-the-evolution-of-phishing.html>.
- [13] Fidelis Security, The RSA Hack, Threat Advisory n. 1001, settembre 2011, <https://archive.orkl.eu/83564e2939b4f62a4ff82c435adba86699cfc753.pdf>.
- [14] United States Department of Justice, Southern District of New York, Lithuanian Man Sentenced to 5 Years in Prison for Theft of Over \$120 Million in Fraudulent Business Email Compromise Scheme, 19 dicembre 2019, <https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business>.
- [15] Agenzia per la cybersicurezza nazionale - CSIRT Italia, Callback Phishing: campagna a tema Polizia di Stato, bollettino BL01/250418/CSIRT-ITA, 18 aprile 2025, <https://www.acn.gov.it/portale/w/callback-phishing-campagna-a-tema-polizia-di-stato>.
- [16] Microsoft Defender Security Research Team, Resurgence of a multi-stage AiTM phishing and BEC campaign abusing SharePoint, 21 gennaio 2026, <https://www.microsoft.com/en-us/security/blog/2026/01/21/multistage-aitm-phishing-bec-campaign-abusing-sharepoint/>.

- [17] Cisco, Security History: The Evolution of Phishing, 6 febbraio 2023, <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m02/security-history-the-evolution-of-phishing.html>.
- [18] Columbia University, School of International and Public Affairs, Target Cyber Attack: A Columbia University Case Study, 2021, <https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf>.
- [19] Lookout, Twitter Phone Spear Phishing Attack, Threat Guidance, luglio 2020, <https://www.lookout.com/documents/threat-reports/us/lookout-twitter-spear-phishing-tg-us.pdf>.
- [20] Microsoft Security Response Center, Threat actor consent phishing campaign abusing the verified publisher process, 31 gennaio 2023, <https://www.microsoft.com/en-us/msrc/blog/2023/01/threat-actor-consent-phishing-campaign-abusing-the-verified-publisher-process>.
- [21] Financial Crimes Enforcement Network (FinCEN), Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004, 13 novembre 2024, <https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf>.
- [22] MGM Resorts International, Current Report on Form 8-K, 5 ottobre 2023, <https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm>; CSHub, A full timeline of the MGM Resorts cyber attack, 15 settembre 2023, <https://www.cshub.com/attacks/news/a-full-timeline-of-the-mgm-resorts-cyber-attack>.
- [23] Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 167, testo vigente al 2026, Normattiva, <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196>.