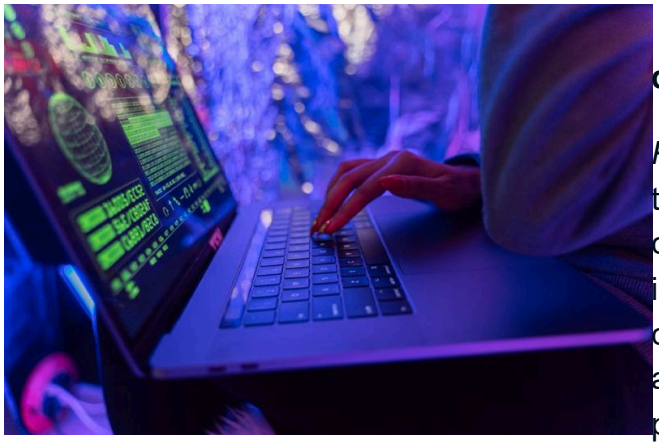
La truffa online su misura: cos’è lo spear phishing e come proteggersi

Autore: redazione

Data: 26/09/2026

Dalla rete a strascico all’arpione digitale: l’evoluzione dello spear phishing



di Alberto Foggia

Pisa, 26 settembre 2026. Il phishing tradizionale opera come una rete gettata alla cieca nel mare digitale: invii massivi e indiscriminati di e-mail generiche, spesso caratterizzate da una sintassi approssimativa, nella speranza che una percentuale minima di destinatari cada nell’inganno inserendo le proprie credenziali bancarie. Lo spear phishing (letteralmente “pesca con l’arpione”) rovescia integralmente questo paradigma.

(foto Antoni Skraba su Pexels)

L’aggressore individua una vittima specifica, ne studia preventivamente il profilo attraverso fonti aperte (social network, registri pubblici), banche dati compromesse circolanti sul dark web o violazioni pregresse di credenziali, e costruisce una trappola personalizzata. Il messaggio contiene riferimenti puntuali e veritieri: l’istituto di credito effettivo, il nome del referente aziendale o del gestore della filiale, ovvero la menzione di fatture e rapporti contrattuali realmente in essere. Quando il bersaglio è un dirigente o un soggetto con poteri di firma societari, la fattispecie assume la denominazione di *whaling*.

Negli scenari più recenti, il fenomeno è mutato radicalmente configurando il "nuovo" spear phishing: una condotta criminale ibrida, multicanale e altamente tecnologica, che non si esaurisce nella mera manipolazione psicologica ma combina vettori di attacco simultanei:

- **intelligenza artificiale generativa e deepfake:** impiego di modelli linguistici per redigere comunicazioni istituzionali prive di difetti ortografici o stilistici, fino alla clonazione vocale (*deepfake audio*) con cui si simulano disposizioni telefoniche urgenti impartite da dirigenti aziendali;
- **spoofing avanzato (Caller ID e SMS spoofing / alias):** alterazione dei metadati di trasmissione in forza della quale l'SMS ingannevole si colloca direttamente all'interno del canale di messaggistica genuino utilizzato dalla banca, mentre la successiva chiamata telefonica (*vishing*) mostra sul display l'esatto numero verde o la linea fissa della filiale;
- **malware hijacking e banker trojan:** la vittima viene convinta a cliccare su un link o a scaricare un finto aggiornamento di sicurezza dell'app bancaria; l'applicazione contraffatta installa un malware che prende il controllo dell'apparato, sopprime o devia le notifiche push e gli SMS alert autentici, e intercetta in tempo reale credenziali statiche e codici dinamici (OTP/XPIN);
- **onboarding e enrollment fraudolento del dispositivo:** mediante l'acquisizione di un singolo codice di autorizzazione temporaneo, gli aggressori collegano l'account di home banking a un nuovo dispositivo sotto il loro esclusivo controllo (*device binding*), esautorando la vittima dalle successive conferme dispositive;
- **SIM swapping e Business Email Compromise (BEC):** duplicazione illecita della scheda SIM della vittima presso i rivenditori telefonici, ovvero intercettazione di caselle di posta elettronica aziendali per alterare le coordinate IBAN delle fatture (*man-in-the-middle*).
-

L'inquadramento penale: i reati e l'importanza della querela

Sul piano penale, lo spear phishing integra un concorso formale di fattispecie criminose a seconda delle condotte esecutive impiegate:

a. Frode informatica (art. 640-*ter* c.p.): costituisce la fattispecie cardine allorché l'aggressore intervenga senza diritto su dati o programmi di un sistema telematico per procurarsi un ingiusto profitto. La norma prevede circostanze aggravanti specifiche: la pena è della reclusione da uno a cinque anni se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale; sale da due a sei anni (con multa da 600 a 3.000 euro) qualora il delitto sia «commesso con furto o indebito utilizzo dell'identita' digitale in danno di uno o piu' soggetti».
b. Truffa contrattuale/telematica (art. 640 c.p.): quando il profitto è conseguito inducendo in errore la vittima tramite artifizi e raggiri volti a ottenere una disposizione patrimoniale.
c. Accesso abusivo a sistema informatico (art. 615-*ter* c.p.): integrato dalla violazione o permanenza non autorizzata nei server dell'istituto bancario o nell'applicativo installato sullo smartphone.
d. Intercettazione e falsificazione di comunicazioni (artt. 617-*ter* e 617-*quater* c.p.): applicabili alle condotte di sniffing, alterazione delle comunicazioni e inoculazione di app-spia.

Sotto il profilo pratico, molte di queste ipotesi delittuose – salvo le fattispecie aggravate – sono perseguibili a querela della persona offesa. La tempestiva presentazione della denuncia-querela presso la Polizia Postale o l'Autorità Giudiziaria non solo preserva la procedibilità dell'azione penale, ma costituisce il presupposto indefettibile per attivare i sequestri preventivi sui conti correnti di destinazione (*money mules*) e ottenere i tracciati telematici utili nel giudizio civile.

Le tutele civili: il regime speciale PSD2 e l'onere della prova della banca

Nel rapporto privatistico tra il cliente e il prestatore di servizi di pagamento (PSP), la materia è disciplinata dal D.lgs. 27 gennaio 2010, n. 11 (di recepimento della Direttiva PSD2). Il legislatore europeo e nazionale ha strutturato un impianto normativo fondato sull'allocazione del rischio d'impresa a carico dell'intermediario.

La tutela del risparmiatore poggia su precisi canoni normativi e giurisprudenziali:

A. Obbligo di rimborso immediato (art. 11 D.lgs. 11/2010)

In presenza di un'operazione non autorizzata, la banca è tenuta a rimborsare il cliente:«immediatamente e in ogni caso al piu' tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo.»

La restituzione con valuta *ex tunc* reintegra la consistenza patrimoniale e neutralizza la maturazione di scoperti di conto o interessi passivi.

B. Inversione dell'onere della prova e diligenza dell'«accorto banchiere» (art. 10 D.lgs. 11/2010)

In deroga all'art. 2697 c.c., l'onere probatorio è posto integralmente a carico dell'intermediario. La giurisprudenza di legittimità ha chiarito in modo costante: «in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo».

La diligenza richiesta al prestatore non è quella dell'uomo medio (art. 1176, comma 1, c.c.), bensì quella professionale qualificata ex art. 1176, comma 2, c.c. dell'«accorto banchiere», che impone l'adozione dei più avanzati presidi tecnologici per prevenire le frodi. Come ribadito dal Collegio di Torino dell'ABF (dec. n. 6052/2021): «ai sensi dell'art. 10 del citato D.lgs. 27 gennaio 2010, n. 11, è onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata, con la conseguenza che, in mancanza di detta prova, l'intermediario sopporta in ogni caso ed integralmente le conseguenze del disconoscimento delle operazioni di pagamento, senza applicazione della franchigia.»

C. L'estensione della prova della SCA: la fase di onboarding e binding dell'app

L'art. 10-*bis* D.lgs. 11/2010 impone l'applicazione dell'Autenticazione Forte del Cliente (*Strong Customer Authentication* – SCA), fondata su almeno due elementi indipendenti riconducibili alle categorie di conoscenza (es. password, PIN), possesso (es. smartphone certificato, token) e inerenza (es. biometria).

Tuttavia, l'orientamento arbitrale e giudiziale più recente ha fissato un principio fondamentale: l'onere della banca di provare la SCA non si limita alla transazione dispositiva finale, ma si estende alla fase propedeutica di installazione, registrazione e associazione del dispositivo (*device onboarding*). Come statuito dall'ABF (Collegio di Bari, dec. n. 1556/2024): «la mancanza di allegazioni relative all'impiego della SCA nella fase di installazione e di configurazione dell'App sul dispositivo del truffatore non consenta di ritenere provata la regolare autenticazione delle operazioni contestate».

La Corte di Giustizia dell'Unione Europea (causa C-409/22, *Eurobank Bulgaria*) ha parimenti sancito che un'autenticazione meramente formale (*prima facie*) o il richiamo a clausole contrattuali non è sufficiente a sollevare il prestatore dalla responsabilità per operazioni non autorizzate.

Il monitoraggio delle anomalie e il ritardo nel blocco operativo

Anche qualora sussista una condotta incauta del risparmiatore, la responsabilità dell'istituto bancario si riespande in caso di negligenza nell'intercettazione dei segnali d'allarme:

Obbligo di SMS Alert e messaggistica informativa: la Suprema Corte (sent. n. 3780/2024) ha confermato la condanna dell'intermediario per non aver dimostrato l'invio tempestivo di alert informativi individuali per ciascuna disposizione. L'ABF (dec. n. 1340/2026) ha stabilito che la mancata attivazione del servizio di alert rende l'istituto responsabile per tutte le operazioni successive alla seconda eseguite a distanza di oltre 5 minuti, in quanto la notifica avrebbe posto la vittima nelle condizioni di bloccare le frodi seriali.

Indici oggettivi di rischio frode (D.M. 30 aprile 2007, n. 112): l'art. 8 del D.M. 112/2007 individua precisi indici sintomatici di rischio (ad esempio, sette o più richieste autorizzative nell'arco di 24 ore per la medesima carta, ovvero plurime disposizioni ravvicinate verso il medesimo IBAN). Il Tribunale di Piacenza (sent. n. 528/2024) ha condannato l'intermediario evidenziando che l'esecuzione di una serie di ricariche ravvicinate da circa 3.000 euro ciascuna su un conto ordinariamente utilizzato per spese minime (€ 100-200) costituisce un'anomalia macroscopica che non può sfuggire al controllo tecnico dell'accorto banchiere.

Ritardo operativo nell'esecuzione del blocco: l'ABF di Bologna (dec. n. 5874/2022) ha censurato il comportamento della banca che, a fronte della richiesta di blocco inoltrata dall'utente via telefono e filiale, ha reso effettivo il blocco solo dopo 23 ore; l'istituto è stato condannato al rimborso integrale di tutte le 20 operazioni fraudolente perfezionate medio tempore.

Il fattore temporale: la segnalazione «senza indugio»

Ai sensi dell'art. 7, comma 1, lett. b) del D.lgs. 11/2010, l'utilizzatore deve comunicare l'uso non autorizzato dello strumento senza indugio non appena ne abbia cognizione, e comunque entro il termine massimo di decadenza di tredici mesi.

La Corte di Giustizia UE (causa C-665/23, *Veracash*, confermata dalle conclusioni dell'Avvocato Generale Medina) ha statuito che la mancata tempestività della comunicazione, se dovuta a dolo o colpa grave dell'utente, preclude il rimborso anche se la contestazione interviene prima della scadenza dei 13 mesi. Al contempo, il ritardo di pochi giorni successivi alla scoperta effettiva della frode non intacca i diritti del correntista (Cass. n. 26916/2020; Trib. Piacenza n. 528/2024).

Guida pratica alla prevenzione per cittadini e imprese

Regole comportamentali:

a) **Nessun intermediario finanziario o forza di polizia richiede telefonicamente o via chat codici OTP, credenziali di accesso, codici PIN o autorizzazioni push.** Chiunque formuli tale richiesta è un truffatore, quand'anche il display del telefono mostri l'esatto numero della banca (*spoofing*).

b) **Non accedere mai a portali bancari tramite link o QR code** ricevuti per messaggio o posta elettronica. Digitare l'indirizzo direttamente nel browser o servirsi esclusivamente dell'applicazione ufficiale.

c) **Interrompere le comunicazioni sospette e richiamare:** in caso di ricezione di messaggi o telefonate allarmistiche su prelievi o blocchi in corso, riagganciare e comporre autonomamente il numero ufficiale dell'assistenza clienti reperibile sul contratto o sulla carta fisica.

d) **Verifica telefonica *out-of-band* per i bonifici societari:** in ambito professionale, prima di dare esecuzione a pagamenti verso nuovi IBAN pervenuti via e-mail o con fatture corrette, contattare l'interlocutore commerciale a mezzo linea telefonica fissa o canale alternativo preventivamente noto.

Presidi tecnici da utilizzare

a) **Autenticazione biometrica e token fisici:** preferire l'autenticazione tramite app con riconoscimento biometrico o chiavi hardware (FIDO2) rispetto all'SMS, maggiormente vulnerabile a intercettazioni e SIM swapping.

b) **Limitazione dei massimali e carte virtuali:** impostare limiti dispositivi giornalieri e mensili ridotti per l'operatività online, utilizzando carte "usa e getta" per gli acquisti su Internet.

c) **Aggiornamento e controllo dei permessi delle app:** mantenere costantemente aggiornati i sistemi operativi e le suite antivirus; non installare file APK o software provenienti da store non ufficiali e non concedere alle applicazioni privilegi speciali di accessibilità o lettura delle notifiche/SMS.

Azioni immediate nelle prime 24 ore e strategia probatoria

a) **Blocco dei canali dispositivi:** contattare immediatamente il servizio antifrode della banca per inibire le carte di pagamento e revocare l'associazione dell'app ai dispositivi mobili.

b) **Cristallizzazione delle evidenze informatiche:** estrarre screenshot integrali dei messaggi ingannevoli, conservare le e-mail con le intestazioni complete (*header* MIME), annotare le numerazioni chiamanti e preservare l'integrità del dispositivo senza procedere a formattazioni premature.

c) **Reclamo formale per iscritto:** trasmettere all'intermediario un reclamo via PEC o raccomandata A/R entro i termini contrattuali, allegando il modulo di contestazione formale delle operazioni, diffidando alla restituzione delle somme ex artt. 10 e 11 D.lgs. 11/2010 e richiedendo l'ostensione integrale dei tracciati informatici di accesso e autorizzazione. La presentazione del reclamo costituisce condizione di procedibilità per il ricorso all'Arbitro Bancario Finanziario.

d) **Richiesta di *recall* per i bonifici:** domandare l'attivazione immediata delle procedure interbancarie di richiamo dei flussi, specialmente per bonifici ordinari non ancora regolati nella stanza di compensazione.

e) **Attenzione processuale ai log bancari (art. 2712 c.c.):** nel contenzioso civile o dinanzi all'ABF, i file di tracciamento prodotti dalla banca costituiscono riproduzioni informatiche che, se non tempestivamente e specificamente disconosciute dalla difesa del cliente nei termini di rito, assumono efficacia di piena prova dei fatti rappresentati circa la regolarità tecnica dell'autenticazione (Corte d'Appello di Milano, sent. n. 696/2026).

Conclusioni

Lo spear phishing contemporaneo costituisce un'aggressione mirata e complessa, capace di dissimulare l'identità istituzionale degli intermediari finanziari attraverso tecnologie di spoofing e infezioni malware. L'ordinamento giuridico predispone una solida rete di protezione che imputa il rischio dell'attività informatica alla sfera professionale della banca. Tuttavia, per garantire il pieno successo della tutela restitutoria, il cittadino deve osservare una rigorosa condotta difensiva: denunciare tempestivamente l'accaduto, conservare scrupolosamente i messaggi ingannevoli (*SMS civetta*) e richiedere l'immediato blocco operativo dei conti compromessi.

*Per approfondire tutti gli aspetti giuridici e pratici legati alle frodi telematiche e alla tutela del correntista, si consiglia la lettura di **«La rete che inganna: truffe online, come difendersi – aspetti pratici e giuridici»**, scritto dall'Avv. Alberto Foggia unitamente ad altri colleghi dell'Associazione ADUSBEF. Il volume è disponibile su Amazon al seguente link: https://www.amazon.it/inganna-difendersi-aspetti-pratici-giuridici/dp/8894863158*