INTESA SANPAOLO

PAGAMENTI DIGITALI E SICUREZZA

Guida per prevenire frodi e truffe

INTESA SANPAOLO

NOTA INTRODUTTIVA

Il progresso tecnologico nell'era digitale ha apportato significativi mutamenti nelle dinamiche sociali. Ai miglioramenti nella facilità e nella velocità di utilizzo dei principali dispositivi di uso comune, come gli smartphone e i pc di ultima generazione, si è purtroppo accompagnata, in tutto il mondo, una crescita dei tentativi di attacco, favorita dalla spesso inconsapevole cessione di informazioni personali riservate da parte dei consumatori.

Il fenomeno frodatorio è estremamente complesso e in costante evoluzione: i frodatori sono diventati sempre più abili nell'adattare il proprio metodo di attacco alle abitudini dei consumatori, per questo è importante conoscere i potenziali pericoli e sapere come proteggersi.

Il presente documento fornisce una panoramica delle principali minacce informatiche e rappresenta una guida sui pagamenti online e con carte e sulle relative frodi e truffe, un "vademecum" utile per supportare la comprensione della materia e della terminologia di riferimento. L'obbiettivo è rendere chiari i passaggi chiave dei processi di pagamento, i fenomeni frodatori e le contromisure adottate dalla banca, al fine di migliorare la consapevolezza sia dei già clienti sia di chi si avvicina per la prima volta ai servizi digitali.
Abbiamo scelto di rendere i contenuti il più possibile accessibili a una vasta platea, sottolineando l'importanza della diffusione della cultura della prevenzione e offrendo in pillole delle informazioni utili atte a prevenire gli attacchi.

La guida è strutturata in tre sezioni principali:

- **un'introduzione al mondo dei pagamenti digitali e delle carte,** in cui sono descritti i processi e gli attori coinvolti e vengono illustrate le principali casistiche di utilizzo;
- **un glossario,** che raccoglie i termini più frequenti che caratterizzano il mondo dei pagamenti, i fenomeni frodatori, le tecniche dei frodatori e le contromisure adottate dalla banca per difendere la clientela dalle minacce quotidiane;
- un breve elenco di **regole di comportamento** per proteggersi dalle frodi e dalle truffe online.

La collaborazione è essenziale per combattere le frodi e le truffe online, per questo è necessario che tutti facciano la loro parte: i clienti stessi, custodendo con cura i dati personali e i codici riservati; le banche, continuando a investire in sicurezza e prevenzione; gli operatori telefonici, verificando scrupolosamente l'identità dei clienti che chiedono un cambio sim e bloccando la manipolazione dei numeri mittenti di telefonate e sms; le Istituzioni nazionali e comunitarie, semplificando la legislazione in materia e consentendo la velocizzazione dei tempi di reazione delle Forze dell'Ordine.

Ci auguriamo che questa pubblicazione, assieme alle pagine dedicate sul nostro sito e alle numerose attività in collaborazione con Istituzioni, Autorità e Associazioni, agevoli la conoscenza delle opportunità e dei rischi del mondo dei pagamenti digitali.

Stefano Lucchini
Chief Institutional Affairs and External Communication Officer

Massimo Proverbio
Chief IT, Digital and Innovation Officer

INTESA SANPAOLO

SOMMARIO

1. IL CONTESTO

1.1. Sistemi di pagamento: categorie principali

Contanti: Uso di moneta e contanti emessi dalle banche centrali.

Pagamenti Internet/Mobile Banking: Transazioni effettuate attraverso l'utilizzo del Web o Mobile Banking.

Carte: Carte di pagamento emesse da istituti finanziari, che consentono l'autorizzazione all'addebito sul conto corrente o l'accesso a una linea di credito.

Real Time Gross Settlement (RTGS): Sistema di trasferimento fondi tramite il quale il denaro viene trasferito da una banca all'altra in tempo reale.

Automated Clearing House (ACH): Network che gestisce le transazioni bancarie elettroniche.
Qualsiasi entità (azienda, organizzazione governativa o individuo) può utilizzare la rete ACH per inviare o ricevere fondi.

Assegni: Titolo di credito attraverso il quale un soggetto (traente) ordina alla banca (trattario) di pagare al portatore legittimo del titolo una somma di denaro esattamente determinata nel titolo.

Nuove forme di pagamento: Pagamenti digitali (es. cryptovalute).

1.2. Principali tipologie di carte

Prepagata – Paga prima

È una carta ricaricabile che consente al Titolare di compiere operazioni tramite i circuiti di pagamento. In particolare, consente di svolgere le stesse operazioni di una carta di credito, ma **possono essere utilizzati solo i fondi precedentemente caricati sulla carta.**
Non è collegata ad un conto bancario o a una linea di credito e il valore dell'acquisto è prelevato immediatamente dalla carta durante la transazione.

Intesa Sanpaolo emette le seguenti tipologie di carte prepagate:

SUPERFLASH

FLASH NOMINATIVA

Debito – Paga ora

La carta di debito è uno strumento di pagamento che permette al Cliente, in base a un contratto con la propria banca, di acquistare beni e servizi presso qualsiasi esercizio aderente ai circuiti ai quali la carta è abilitata o di prelevare contante con addebito immediato sul conto corrente collegato alla carta.

Una carta di debito **ha accesso solo ai fondi disponibili sul conto del titolare ed entro i limiti operativi previsti dalla carta medesima.**

Per ottenerla è sufficiente avere un conto in banca, non è necessario un credit check.

Intesa Sanpaolo emette le seguenti tipologie di carte di debito:

EXCLUSIVE DEBIT

XME DEBIT CARD

Credito – Paga dopo

La carta di credito consente, entro il massimale di spesa mensile ed entro i limiti specifici per i prelievi di contante indicati sul contratto, di compiere operazioni tramite i circuiti di pagamento convenzionati.

Offre a clienti e imprese linee di credito di breve periodo e varie opzioni di rimborso.

Dà la possibilità di acquistare beni e servizi **senza prelevare immediatamente fondi.** Il pagamento è differito e avviene, solitamente, a cadenza mensile e in un'unica soluzione per l'importo complessivo speso nel mese precedente.

La banca dell'esercente ottiene fondi dalla banca del titolare della carta e l'emittente della carta invia un bilancio al titolare con la periodicità indicata nel contratto.
Intesa Sanpaolo emette le seguenti tipologie di carte di credito:

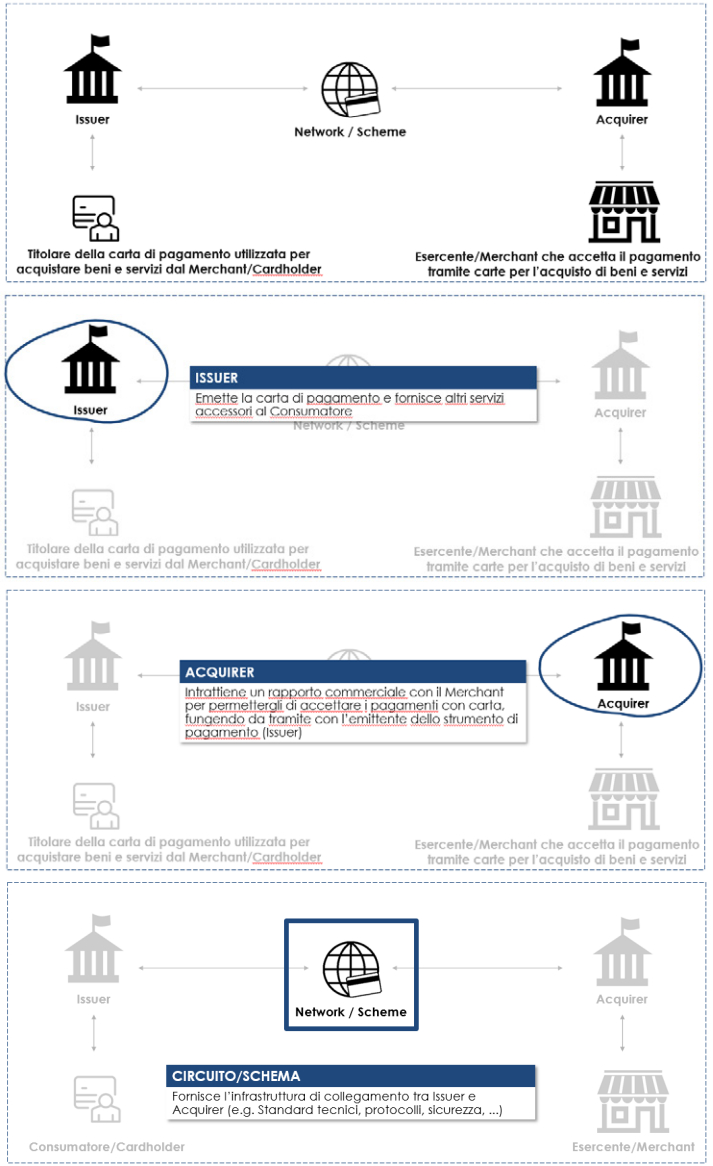
CLASSIC CARD

GOLD CARD

EXCLUSIVE CARD

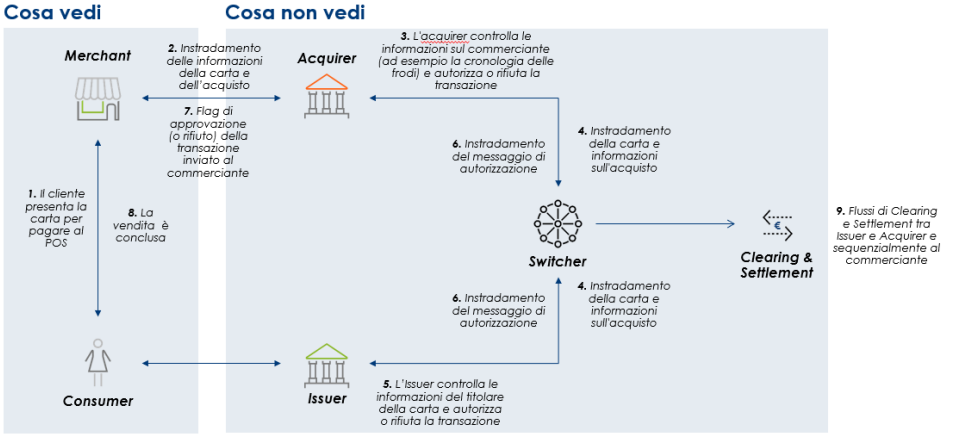
1.3 Modello a 4 parti: panoramica

Il modello “a 4 parti” presuppone l’intervento dei seguenti quattro soggetti: consumatore (Titolare della carta); emittente della carta (Issuer); esercente (Merchant); banca dell’esercente (Acquirer).



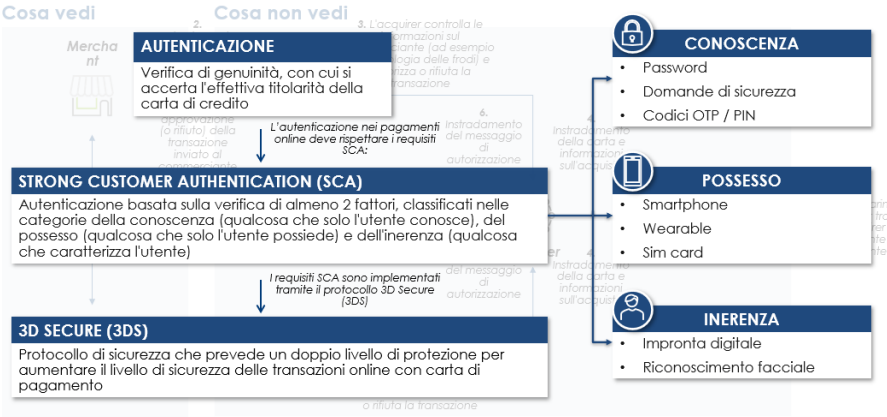
1.3.1 Modello a 4 parti: come funziona tecnicamente una transazione

In una transazione con carta di pagamento sono coinvolti tutti gli attori del modello a 4 parti.



1.3.2 Modello a 4 parti: Autenticazione

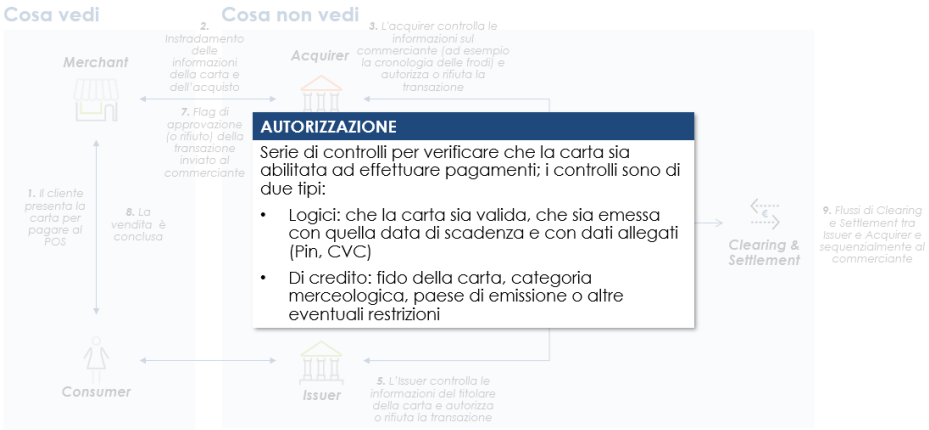
Autenticazione e Autorizzazione sono fasi di verifica obbligatorie che precedono il pagamento vero e proprio.



*Card Verification Value (CVV, CVV2, CVC2): codice di sicurezza stampato sul retro della carta e composto dalla combinazione numerica di tre o quattro cifre. Il codice è richiesto negli acquisti online per verificare che la persona che effettua il pagamento sia effettivamente in possesso della carta.

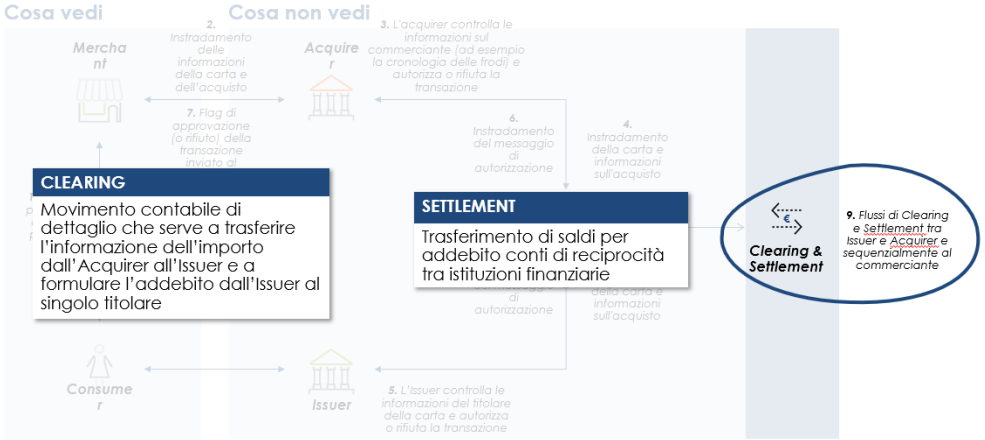
1.3.3 Modello a 4 parti: Autorizzazione

Autenticazione e Autorizzazione sono fasi di verifica obbligatorie che precedono il pagamento vero e proprio



1.3.4 Modello a 4 parti: Clearing & Settlement

Clearing e Settlement sono le ultime fasi del processo di pagamento, dove i fondi vengono effettivamente trasferiti tra istituti finanziari



1.4 Processo di Pagamento: panoramica

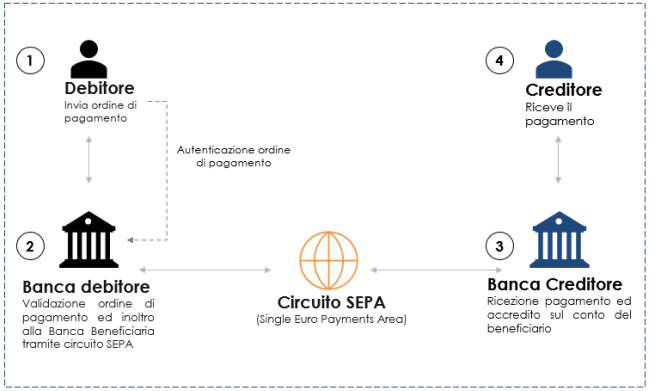
Di seguito un esempio del processo di pagamento tramite bonifico SEPA

Bonifico SEPA – Definizione[1]

Ordine dato dal **debitore** di trasferire una somma sul conto di un **creditore**, di norma con addebito sul proprio conto corrente.

Per effettuare un SCT è necessario fornire obbligatoriamente il **codice IBAN** del beneficiario, che identifica in modo univoco il conto di destinazione dei fondi.

Dal 1° agosto 2014 lo standard utilizzato per i bonifici in Euro è quello del bonifico europeo (SEPA credit transfer - SCT).



[1] *Fonte: Banca D'Italia - https://www.bancaditalia.it/compiti/sispago-mercati/strumenti-pagamento/index.html*

2. PRINCIPALI CASISTICHE DI UTILIZZO NEL MONDO DEI PAGAMENTI

I principali utilizzi possono essere distinti tra pagamenti **card present, pagamenti card not present e prelievi ATM.**

2.1 Pagamenti Card Present (CP)

I pagamenti **card present (CP)** si differenziano tra pagamenti **contactless**, pagamenti **Chip&Pin** e **Swipe.**

- In una transazione «card present» il cardholder dispone il pagamento direttamente presso l'esercente, utilizzando i circuiti di pagamento della carta.
- Durante una transazione Card Present, **la carta può essere letta in diverse modalità:**
  - Contactless (inclusi anche i casi in cui viene utilizzato un wallet di pagamento installato su un device, in sostituzione della carta fisica);
  - POS (Chip&Pin) - con inserimento del chip nell'apposito lettore (EMV);
  - Swipe (banda magnetica).

2.1.1 Pagamenti Contactless

Il sistema di pagamento **contactless** permette di effettuare acquisti tramite carte di pagamento **senza contatto.**

- Una carta contactless è una **carta con chip con tecnologia incorporata che consente di pagare tramite un'interfaccia radio (RFID),** senza la necessità di leggere il contenuto della carta a mezzo di contatto col lettore.
- La carta di pagamento può anche essere **digitalizzata** come token **sul digital wallet di un device** (es. smartphone e wearable) **che utilizza l'antenna NFC per pagamenti contactless** (es. Apple Pay, Google Pay, Garming, Fitbit, ...)
  - **Tokenizzazione:** processo mediante il quale i dati della carta vengono asso ciati ad un Digital Wallet.
  - **Digital wallet:** app o altri servizi on-line che memorizzano le versioni virtuali (token) delle carte di debito e credito.

2.1.2 Pagamenti Chip&PIN

La tecnologia **Chip&PIN** sostituisce l'utilizzo della banda magnetica e della firma per i pagamenti con moneta elettronica.

- EMV chip è una tecnologia di cui possono essere dotate le carte di pagamento, che consente sia di **combattere i rischi di frodi e clonazione, sia di proteggere i dati di pagamento sensibili in ambito «card present».**
- Supporta l'autenticazione dinamica (**dynamic linking:** requisito di sicurezza che prevede un codice univoco di autenticazione specifico per l'importo dell'operazione e il beneficiario, utilizzabile per una sola transazione).
- La carta EMV è una carta che **deve essere inserita nel lettore POS e richiede l'inserimento del PIN per poter effettuare il pagamento.**

2.2 Pagamenti Card Not Present (CNP)

I pagamenti **card not present (CNP)** si differenziano tra pagamenti **E-commerce, Recurring e MIT/MOTO.**

- Una transazione **«card not present»** si ha quando il titolare della carta **non presenta fisicamente la carta** a un commerciante al momento dell'ordine e del pagamento effettuato.
- Per ridurre il rischio di frodi in un pagamento CNP è possibile creare una **carta virtuale** usa e getta o con durata prestabilita, che presenta un **numero di carta fittizio** da utilizzare in **sostituzione di quello riportato sulla carta fisica.**

2.2.1 Pagamenti E-commerce

I pagamenti **e-commerce** passano tramite un gateway di pagamento, che gestisce il flusso elettronico.

- I pagamenti E-commerce consistono **nell'acquisto online di beni e/o servizi tramite una transazione commerciale** che vede l'uso di un device (strumento) che trasmette i dati della carta o di un suo token.
- I dati vengono tramessi **tra i siti di e-commerce e gli acquirenti** tramite gateway di pagamento.

2.2.2 Pagamenti Recurring

I pagamenti ricorrenti consistono nell'**addebito ripetuto** (ogni mese) di una somma sempre uguale per un periodo di tempo prestabilito.

- Un pagamento ricorrente avviene a seguito di un **accordo tra un titolare di una carta di pagamento e un commerciante in cui si autorizza quest'ultimo ad addebitare il conto del titolare della carta su base continuativa,** senza una data di fine specificata.

2.2.3 Pagamenti MIT/MOTO

I pagamenti **MIT/MOTO** sono avviati dal commerciante previa autorizzazione del cliente o tramite ordine per corrispondenza/telefono.

- **MIT: Merchant Initiated Transaction,** sono **pagamenti avviati dal commerciante** che in base a un accordo stipulato con il cliente, dispone il pagamento per suo conto.
  - Es. attività in abbonamento con futuri pagamenti mensili di importi variabili.
- **MOTO: Mail Order/Telephone Order,** sono t**ransazioni avviate tramite ordine per corrispondenza o per telefono** a mezzo di inserimento manuale del numero della carta, scadenza e codice di sicurezza, senza la presenza fisica dell'acquirente.
  - Es. vendita di un prodotto a distanza.

3. DIFFERENZA TRA FRODE E TRUFFA

FRODE[1]: Emissione di un ordine di pagamento da parte del frodatore.

Si tratta di **operazioni di pagamento non autorizzate dal titolare dello strumento di pagamento** ma effettuate dal frodatore, in conseguenza dello **smarrimento**, del **furto** o dell'**appropriazione indebita** di dati relativi allo strumento di pagamento.

Esempi:

Phishing
SIM swap
Malware

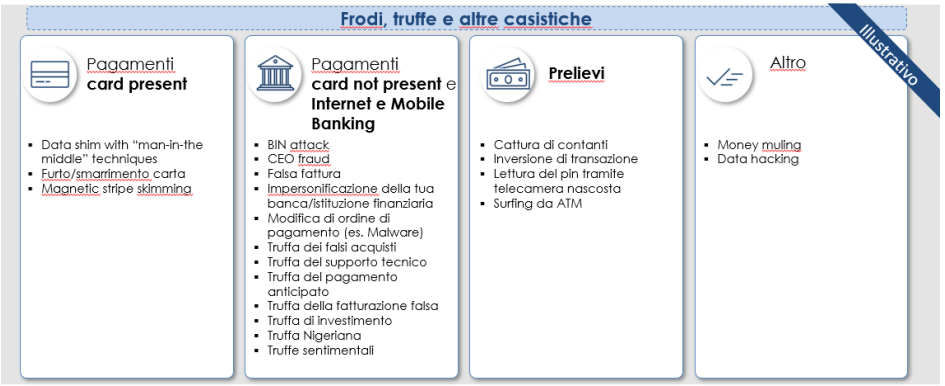
TRUFFA[2]: Manipolazione operata dal frodatore a danno del pagatore allo scopo di indurlo a emettere un ordine di pagamento.

Si tratta di **operazioni disposte dal titolare dello strumento di pagamento in favore del truffatore a causa di una manipolazione operata da quest'ultimo** («manipolazione del pagatore»).

Esempi:

Truffe sentimentali
Truffa dei falsi investimenti
CEO fraud
Truffa Nigeriana

3.1 Esempi di frodi e truffe



1 Fonte: Guidelines on fraud reporting (EBA GL-2018-05) - https://www.eba.europa.eu/
2 Fonte: Guidelines on fraud reporting (EBA GL-2018-05) - https://www.eba.europa.eu/

4. GLOSSARIO

A

Account Takeover Fraud
L'account takeover è una forma di furto di identità online in cui una terza parte accede in modo illegittimo all'account di una vittima modificandone i dettagli, effettuando acquisti e sfruttando le informazioni rubate per accedere ad altri account.

Adware
è una tipologia di malware che si nasconde sui dispositivi ed è programmato per raccogliere informazioni sulle operazioni effettuate dall'utente e per visualizzare periodicamente messaggi pubblicitari non richiesti.

Antivirus
Software che intercetta eventuali attacchi o riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli.

Attacco Man in the middle (MitM)
Attacco informatico in cui l'hacker si intromette tra il cliente e le attività che svolge online, come ad esempio attività sul sito di online banking, e-mail di lavoro, immissione di dettagli di pagamento e così via.

Autenticazione forte del cliente (SCA - Strong Customer Authentication)
Autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri.

Authorized push payment fraud
Casi in cui un soggetto o un'organizzazione vengono indotti con l'inganno ad autorizzare un pagamento verso un beneficiario ritenuto "affidabile", dietro cui si nasconde un truffatore.

B

Banca
Istituto che compie operazioni monetarie e di credito, svolgendo congiuntamente e in modo consequenziale attività di raccolta del risparmio e di concessione del credito.

Beneficiario
Il soggetto previsto quale destinatario dei fondi oggetto dell'operazione di pagamento.

BIN attack
Un attacco BIN prevede che un truffatore prenda i primi sei numeri di una carta (il numero di identificazione della banca o BIN) e, utilizzando un software, genera automaticamente i numeri rimanenti e verifica queste combinazioni per vedere quali numeri di carta sono corretti e se le carte sono attive.

C

Cattura di contanti
La cattura di contanti è un tipo di frode in cui il frodatore attraverso la manomissione dell'ATM tramite specifici dispositivi cattura i contanti dei clienti che eseguono operazioni di prelievo.

CEO Fraud
La truffa del CEO si verifica quando un soggetto, fingendosi una figura di alto livello all'interno dell'azienda (ad esempio CEO o CFO), individua e induce, tramite ad esempio chiamate o e-mail, un dipendente autorizzato a effettuare un pagamento dall'account aziendale verso un conto controllato dal truffatore.

Chargeback
Il chargeback è una procedura attraverso la quale un consumatore può annullare il trasferimento di denaro effettuato a favore di un esercente se ha riscontrato dei problemi nella transazione.

Chiamate da finti operatori bancari / istituzioni finanziarie fasulle
Le chiamate da finti operatori bancari o finte istituzioni finanziarie sono truffe che implicano telefonate o messaggi in cui i frodatori affermano di provenire da società di servizi postali, banche o agenzie governative, spingendo ad agire su una questione che richiede attenzione immediata e creando un senso di urgenza.

Clonazione carta
Si verifica quando il frodatore utilizza le informazioni della carta originale per creare una copia della carta della vittima.

Codice Malevolo
Si parla di codice malevolo per indicare una serie di dati che rappresentano istruzioni potenzialmente dannose.

Compromissione e-mail aziendale
La compromissione dell'e-mail aziendale è una modalità di attacco in cui il truffatore, dopo aver compromesso l'e-mail aziendale della vittima, intercetta le comunicazioni e, fingendo di essere un fornitore ufficiale dell'azienda, richiede una modifica dell'IBAN o invia una fattura alterata per poter ricevere pagamenti su un conto che controlla.

Conto corrente
Il conto corrente bancario è un prodotto che consente incassi e pagamenti utilizzando i fondi depositati dai clienti o accordati dalla banca con un finanziamento. Al conto corrente è possibile accedere tramite inserimento delle credenziali (Codice Titolare e PIN) su piattaforma Web o Mobile Banking.

Conto Di Pagamento
Un conto intrattenuto dal pagatore presso un istituto di credito che consente di effettuare incassi e pagamenti (ad es. conto corrente, carta prepagata con IBAN in ingresso ed in uscita).

Cookie
I cookies sono piccoli file di testo che conservano scelte, opzioni e selezioni degli utenti fatte sui siti internet. Ci sono cookies utili alla gestione della navigazione e altri che tracciano le nostre abitudini comportamentali, come ad esempio per gli acquisti on-line.

Crimine cibernetico (Cyber-Crime)
Qualsiasi reato o comportamento delittuoso svolto nell'ambito delle procedure informatiche.

Criptovalute (Crypto)
Una criptovaluta è una valuta virtuale che costituisce una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le criptovalute possono essere trasferite, conservate o negoziate elettronicamente.

Crittografia
Tecnica che permette di nascondere il contenuto di un messaggio, in modo che esso possa essere correttamente compreso solo da chi ne possiede la chiave di decifrazione.

Cyber-Attacco
Si riferisce ad una manovra di attacco informatico da parte di uno o più individui verso un sistema, con la finalità di accedere, modificare, distruggere o rubare informazioni e dati.

Cyberspazio - Spazio cibernetico (Cyber-Space)
L'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi.

D

Dark web
Contenuti del web nelle darknet (reti oscure) che possono essere raggiunti esclusivamente con software specifici.

Data hacking
Furto di dati sensibili che può determinare l'"Account Data Compromise".

Data shim with «man-in-the-middle» techniques
Tecnica di captazione dei dati della banda magnetica presenti nel chip attraverso la manomissione del terminale EMV.

Denial of Service (DDoS)
Attacco DoS lanciato da un gran numero di sistemi compromessi e infetti (botnet), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

Disputa
Tutte le transazioni contestate da un cliente, per le ragioni più svariate.
Ad esempio, si può avviare una disputa per frode, per servizio non reso o non conforme o per ragioni tecniche di addebito non corretto.

E

Encryption
Crittografia dei dati, che si effettua a mezzo di chiavi conosciute dalle parti. La crittografia si suddivide spesso in pubblica e privata, a seconda delle chiavi usate.

F

Falsa fattura
Si tratta di un tipo di truffa in cui un'azienda viene contattata da un falso creditore che fornisce le nuove coordinate bancarie per il pagamento della fattura. Possono essere utilizzati vari approcci in combinazione tra loro: telefono, lettera, e-mail, ecc. Il truffatore richiede che vengano modificate le coordinate bancarie per il pagamento delle fatture future (ad esempio i dettagli del beneficiario del conto bancario).

False Decline
Termine tecnico usato per misurare i rapporti di efficacia dei sistemi di fraud detection. Uno degli indicatori usati misura i "falsi positivi", cioè il numero dei alert che è necessario generare prima di individuare una transazione fraudolenta, a mezzo indici di anomalia. Il false decline è una transazione genuina che viene negata a un cliente in quanto la probabilità di frode data dall'insieme di regole e algoritmi del sistema di controllo è molto elevata.

Fattore Umano
Nella sicurezza informatica l'intervento dell'uomo è determinante per proteggersi dalle frodi. L'insieme delle buone norme di condotta da adottare da parte degli individui o delle organizzazioni è un aspetto cruciale per prevenire o attenuare le conseguenze degli attacchi.

Furto carta
Si verifica quando avviene la "Sottrazione fisica" della carta alla vittima e l'utilizzo della stessa per acquisti, pagamenti o prelievo dei fondi presso ATM.

Furto di dati (Data Theft)
È l'atto di sottrarre informazioni. Questa forma di furto aziendale è un rischio significativo per le aziende di tutte le dimensioni e può avere origine sia all'interno che all'esterno di un'organizzazione.

Furto d'identità
Si intende il furto dei tuoi dati personali (ad esempio nome, codice fiscale, numero di carta di credito, CVV, ecc.) per scopi fraudolenti.

Fraudolent application
Si verifica quando viene richiesta l'emissione di una carta di pagamento da parte del frodatore utilizzando il nome e le informazioni reali di un'altra persona.

Friendly Fraud
Frode effettuata dallo stesso cliente o dal suo "inner circle". Si divide in due sottocategorie: la frode in buona fede, dove il cliente dichiara di non aver fatto l'operazione ma in realtà l'ha fatta qualcuno a lui vicino che ha accesso ai dati (figli o persone a lui vicine)

e la frode dove il cliente scientemente dichiara il falso (spesso su operazioni di piccolo importo, semplicemente per non pagare il bene, o il servizio, di cui ha usufruito).

Frode della Bolletta
Il frodatore, promuovendo campagne di risparmio sul pagamento delle bollette tipicamente tramite siti o annunci falsi, convince un soggetto A, ingannato dal risparmio promesso e inconsapevole di essere complice di una truffa, ad inviare i dati della propria bolletta da pagare. Il frodatore, utilizzando le credenziali bancarie carpite tramite ingegneria sociale da un altro soggetto B (vittima della frode), effettua dal conto di quest'ultimo il pagamento della bolletta del soggetto A. Una volta conclusa l'operazione, il frodatore invia al soggetto A la ricevuta del pagamento per farsi corrispondere l'importo pattuito.

H

Hacker
L'hacker è un soggetto esperto dei sistemi informatici e dei software. Si distingue in:

- **Black-hat hacker:** viene definito black-hat chi si introduce illegalmente nei sistemi informatici con l'obiettivo di appropriarsi illecitamente di informazioni o provocare un danno;
- **White-hat hacker:** viene definito "white-hat", un hacker esperto di program mazione e sicurezza informatica, in grado di introdursi nei sistemi di reti con l'obiettivo di aiutare i proprietari di quel sistema a scoprire eventuali falle nell'accesso, valutarne l'affidabilità, e risolvere potenziali problemi di sicurezza.

HTTP
L'HyperText Transfer Protocol, ovvero il protocollo di trasferimento di un ipertesto, è un protocollo, uno standard, usato come principale sistema per trasferire informazioni sul web. L'HTTP si basa su un sistema di comunicazione tra "client" e "server": il client esegue una richiesta e il server restituisce la risposta. Nell'uso comune il client corrisponde al browser con cui si naviga su Internet (ad esempio Chrome, Edge, Firefox, Opera, Safari), il server è la macchina su cui risiede il sito web.

HTTPS
Aggiungendo una "S", che racchiude il significato di Sicurezza, al protocollo HTTP, otteniamo l'HTTPS. Questo è infatti protocollo per la comunicazione attraverso una rete di computer utilizzato su Internet, all'interno di una connessione sicura, criptata. HTTPS permette di verificare che il sito visitato sia autentico, fornisce una protezione maggiore della privacy e garantisce che i dati scambiati tra l'utente e il sito web non vengano intercettati o manomessi.

I

Impersonificazione della tua Banca/ Istituzione finanziaria
Avviene nel momento in cui un truffatore si finge la tua banca o un'istituzione finanziaria. Solitamente il fine è quello di indurre il cliente a trasferire denaro su un altro conto che in realtà controlla lui.

Indirizzo IP
È un codice univoco, composto da quattro set di cifre comprese tra 0 e 255 che identifica ogni dispositivo.

Ingegneria sociale
Tecniche di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Intelligenza Artificiale (AI – Artificial Intelligence)
Disciplina che si occupa dello studio di funzioni tipiche dell'intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.

Intercettazione della carta in transito (boxing)
Si intende solitamente la sottrazione della carta "fisica" durante la spedizione al legittimo cliente per utilizzi fraudolenti. Si parla anche di Never Received or Issue (NRI).

Inversione di transazione
È un tipo di frode in cui il frodatore manomette l'ATM per intrappolare la carta e interrompere l'operazione di prelievo. In realtà, il processo è andato a buon fine e il frodatore, una volta che il cliente si allontanato dall'ATM, procede al ritiro del contante.

L

Landing Page
Landing Page è la prima pagina di un sito web che il visitatore raggiunge dopo aver cliccato un link.

Login
Procedura di autenticazione con cui si accede a una sezione riservata di un sito Internet.

M

Magnetic stripe skimming
Clonazione dei dati carta presenti nella banda magnetica, generalmente a mezzo lettura e copiatura integrale della stessa.

Malware
Software malevolo inserito in un sistema informatico con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi.

Manipulation of Cardholder
Qualsiasi transazione di pagamento effettuata a seguito della manipolazione del pagatore da parte del truffatore.

Merchant Fraud
Frode commessa dall'esercente, in gererale si divide in due sottocategorie: bust-out o senza. Lo schema di bust-out prevede una collusione dell'esercente con i titolari di carte di pagamento, in quanto questi ultimi non metteranno a disposizione dell'issuer i fondi necessari per compensare le spese effettuate con la carta. Lo schema non bust-out si basa sull'uso illecito di carte, senza connivenza con il titolare (ad esempio, finti negozi online che, dopo aver accettato i pagamenti, non evadono gli ordini).

Minaccia Cibernetica
Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi.

Minacce persistenti avanzate (APT – Advanced Persistent Threat)
L'APT è un tipo di attacco informatico in cui si utilizzano sofisticate tecniche di hacking al fine di ottenere l'accesso ad un sistema e rimanere all'interno per tempi prolungati.

Mirroring
Creazione di un sito clone della banca o dell'istituzione finanziaria. È spesso usato nelle mail di phishing dove il cliente clicca su un link attivo che lo indirizza al sito clone dove gli viene richiesto di inserire le credenziali di accesso al fine di carpirle. Dopo l'inserimento, in genere la sessione operativa in uso del cliente restituisce un messaggio di errore tecnico.

Modification of Payment Order
Si riferisce a una situazione in cui il frodatore intercetta e modifica un ordine di pagamento legittimo durante la comunicazione elettronica tra il dispositivo del pagatore e il prestatore di servizi di pagamento. Tale tipologia di frode viene perpetrata, ad esempio, attraverso malware o attacchi che consentono agli aggressori di intercettare la comunicazione tra due host che comunicano legittimamente (attacchi man-in-the middle).

Money Muling
È un tipo di truffa in cui un soggetto viene reclutato per riciclare denaro ottenuto attraverso attività illecite. Tipicamente i malfattori reclutano i titolari di un conto bancario, tramite tecniche di inganno sociale tra cui false offerte di lavoro o prospettando facili guadagni movimentando denaro trasformandoli in "money mule".

N

Nome utente (Username)
Il nome identificativo dell'utente che è normalmente visibile, diversamente dalla password.

P

Pagatore
Soggetto titolare di un conto di pagamento a valere sul quale viene impartito un ordine di pagamento ovvero, in mancanza di un conto di pagamento, il soggetto che impartisce un ordine di pagamento.

Phishing
Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (user id, password, numeri di carte di credito, CVV, PIN) con l'invio di false e-mail. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fasulli.

PIN (Personal Identification Number)
Sequenza di caratteri nota solo al legittimo proprietario; la sua introduzione consente l'accesso al proprio Internet Banking e permette di autorizzare le transazioni.

Pin reading with hidden camera
Tecnica in uso soprattutto presso gli ATM, dove viene posizionata una telecamera per spiare il pin del cliente. Può esserci una falsa tastiera sovrapposta all'originale e il tutto viene abbinato alla captazione dei dati della banda magnetica tramite skimmer.

PSD2 (2015/2366/UE)
La PSD2 è la direttiva europea sui servizi di pagamento. Nel mercato interno essa mira a regolamentare i servizi di pagamento e i gestori dei servizi di pagamento all'interno dell'Unione europea, promuove lo sviluppo di un mercato interno dei pagamenti al dettaglio efficiente, sicuro e competitivo e rafforza la tutela degli utenti dei servizi di pagamento, sostenendo l'innovazione e aumentando il livello di sicurezza dei servizi di pagamento elettronici.

Q

QR code fraud
È una variante del phishing, dove al posto di un link viene inviato alla vittima della frode un QR code, oppure la richiesta di inquadrare un QR code per ricevere un pagamento. Il QR code inquadrato dalla vittima, invece, avvierà una app di pagamento oppure installerà un software malevolo (malware) sul device utilizzato.

R

Ransomware
Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica.

S

Sextortion
Il sextortion (dall'inglese "sexual" + "extortion") è una truffa online che mira a estorcere denaro alle vittime attraverso ricatti sessuali effettuati sui social network o con finte e-mail minatorie.

Shoulder Surfing da ATM
Semplice tecnica di spiare il codice pin digitato su un ATM.

Sicurezza cibernetica (Cyber-Security)
Condizione in cui il cyber-space risulti protetto rispetto a eventi, di natura volontaria od accidentale, grazie ad idonee misure di sicurezza fisica, logica e procedurale.

SIM Swap
Consiste nella duplicazione della scheda SIM del cliente rilasciata illecitamente ai truffatori dai gestori di telefonia mobile. Con tale tecnica, i truffatori intercettano gli sms contenenti i codici dispositivi inviati dalla banca al cliente e li utilizzano per disporre operazioni fraudolente.

Sistemi di monitoraggio antifrode
Sistemi dedicati all'analisi e al blocco delle operazioni sospette al fine di individuare le operazioni ritenute a rischio di frode.

Smartphone
Tipo di telefono cellulare che, oltre alle funzioni di telefono, integra la gestione di dati personali, il collegamento a Internet, la posta elettronica, ecc.

Smishing
Lo smishing (dalla combinazione delle parole SMS e Phishing) è il tentativo da parte dei frodatori di acquisire informazioni personali, finanziarie o di sicurezza tramite link inviati via SMS.

Spam
Messaggi di posta elettronica indesiderati, generalmente pubblicitari o malevoli.

Spoofing
Attacco informatico in cui un mittente sconosciuto finge di essere un mittente conosciuto e considerato attendibile dal destinatario.

Spyware
Tipo di software malevolo che "spia" le attività in rete di un utente per carpirne codici, azioni, ecc.

T

Threat actor
Espressione impiegata per indicare singoli individui o organizzazioni il cui fine è distruggere, danneggiare od ostacolare il regolare funzionamento dei sistemi e delle reti, ovvero a violare l'integrità e la riservatezza di dati/informazioni.

Transazione
Operazione di pagamento effettuata fisicamente o da remoto.

Trojan Horse
Tipo di software malevolo, che si annida nel PC ospite camuffandosi da programma innocuo.

Truffa dei Falsi acquisti
Sono truffe in cui si utilizzano pubblicità di prodotti o servizi in vendita su siti web o su siti di aste online al fine indurre all'acquisto i clienti che non riceveranno mai il prodotto o il servizio acquistato. Il venditore richiede il pagamento tramite trasferimento di denaro e l'acquirente non riceve mai la merce.

Truffa del supporto tecnico
È un tipo di truffa in cui il criminale, fingendo di essere un tecnico informatico, convince il cliente a cedere informazioni o a effettuare download di programmi o di applicazioni, che consentono l'accesso del truffatore ai dispositivi del cliente.

Truffa del pagamento anticipato
La truffa del pagamento anticipato è un tipo di truffa in cui la vittima viene convinta a effettuare un pagamento anticipato (es. una tariffa) necessario per la consegna di beni di elevato valore, rivelatisi poi inesistenti.

Truffa della fatturazione falsa
Sono truffe in cui alla vittima viene richiesto il pagamento di una o più fatture emesse per l'acquisto di beni o servizi mai richiesti.

Truffa di investimento
Si realizza nei casi in cui il truffatore contatta la vittima proponendo investimenti tramite false società finanziarie poi rivelatesi inesistenti o, comunque, inadempienti rispetto alla domanda di restituzione delle somme.

Truffa Nigeriana
Si verifica nei casi in cui un soggetto truffatore (solitamente estero) offre alla vittima la quota di una somma di denaro in cambio del pagamento di false commissioni o presunte tasse.

Truffa sentimentale
È una forma particolare di cyber-truffa, ossia di raggiro volto all'ottenimento illecito di denaro, utilizzando Internet come mezzo privilegiato di interazione con la vittima.

U

URL
Sequenza di caratteri che identifica in modo univoco l'indirizzo Internet di una pagina, di un documento o di una risorsa.

V

Violazione dei dati (Data Breach)
Nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone.

Virus
Software malevolo che può infestare un PC, inserendosi in un programma applicativo, causando danni diretti o indiretti, e che può propagarsi da questo ad altri PC tramite file condivisi, e-mail, ecc.

Virtualizzazione fraudolenta della carta
Implica la digitalizzazione della carta da parte del frodatore sul proprio dispositivo (es. su wallet di Apple Pay, Google Pay) attraverso l'intercettazione dei dati della carta e dei codici inviati dalla banca al cliente al fine di effettuare acquisti fraudolenti.

Vishing
Il vishing (dalla combinazione delle parole Voice e Phishing) è il tentativo da parte dei frodatori di acquisire informazioni personali, finanziarie o di sicurezza, identificandosi al telefono come operatori della banca.

VOIP (Voice Over IP): Protocollo che permette la trasmissione in Internet, con protocollo IP, della voce. Permette di ottenere la fonia su Internet.

W

Web
Servizio di Internet che permette di navigare e di usufruire dei contenuti multimediali della Rete.

Worm
È un malware che, dopo aver compromesso un PC, è in grado di autoreplicarsi e di diffondersi all'interno di una rete locale per infettare gli altri dispositivi connessi.

INDICE DEL GLOSSARIO

5. PRINCIPALI REGOLE PER DIFENDERSI DALLE FRODI ONLINE

1) Non cliccare su link fasulli forniti via e-mail o SMS.
Controlla attentamente l'indirizzo del mittente delle e-mail: se sembra provenire dalla banca, verifica che l'indirizzo contenga @intesasanpaolo.com. In ogni caso, la banca non invia mai link all'interno di SMS ed e-mail che rimandano a pagine web in cui è necessario inserire le proprie credenziali di accesso al servizio di e-banking (Codice Titolare e PIN). Non aprire e cestina messaggi ed e-mail che richiedono i codici personali o di compiere un'azione con urgenza.

2) Verifica il link dell'Internet Banking ufficiale.
Accedi al sito internet della banca digitando tu stesso l'indirizzo web (URL) di riferimento nella barra di ricerca del browser (ad esempio www.intesasanpaolo.com), oppure controlla la correttezza dell'indirizzo web, anche passandoci sopra il mouse senza cliccare (protocollo https, dominio, indirizzo complessivo: ad esempio: https://www.intesasanpaolo.com/).

3) Verifica i numeri di telefono in entrata.
Ricorda che il Numero Verde della banca è attivo solo per ricevere chiamate, non per effettuarle. Se hai dei sospetti in merito a delle chiamate ricevute, chiama tu il Numero Verde o la tua filiale per verificare l'attendibilità del numero che ti ha chiamato o del mittente di un SMS.

4) Non cedere i tuoi codici personali a terzi e nemmeno alla banca.
La banca non ti contatterà mai per chiederti i tuoi codici bancari e di sicurezza o per effettuare delle operazioni di pagamento per simulazioni o storni. Cambia frequentemente il PIN evitando di utilizzare codici già usati in precedenza o troppo semplici o ricavabili facilmente dai tuoi dati anagrafici.

5) Presta attenzione quando installi le APP.
Installa tutte le app scaricandole solo dagli store ufficiali (Google Play Store, Apple Store e Huawei AppGallery). Non installare mai software su richiesta telefonica, né tramite link ricevuti via SMS o e-mail. Non scaricare gli allegati ricevuti da numeri o mittenti sconosciuti se non sei sicuro della loro legittimità, perché potrebbe trattarsi di un malware.

6) Assicurati di avere sempre un antivirus installato sul tuo dispositivo ed effettua regolarmente gli aggiornamenti di sistema e delle applicazioni.

7) Prima di confermare un'operazione, controlla sempre che gli IBAN dei beneficiari mostrati nella schermata di riepilogo siano quelli da te inseriti.

8) Rimani sempre aggiornato rispetto alle truffe più recenti per riconoscerle in tempo

Per avere maggiori informazioni sulle frodi online bancarie e i cyber attacchi più comuni, consulta periodicamente la pagina di Sicurezza che trovi sul sito: www.intesasanpaolo.com.

BIBLIOGRAFIA / SITOGRAFIA DI RIFERIMENTO

INTESA SANPAOLO
https://www.intesasanpaolo.com/
https://www.intesasanpaolo.com/it/persone-e-famiglie/bisogni/sicurezza-digitale/phishing-bancario.html

Cyberbook
www.sicurezzanazionale.gov.it
www.beawarebedigital.gov.it

E.A.S.T. European Fraud Update
https://www.association-secure-transactions.eu/

CERTFin
https://www.certfin.it/

Mastercard
https://www.mastercard.it/

ENISA
https://www.enisa.europa.eu/

BANCA D'ITALIA
https://www.bancaditalia.it/footer/glossario/index.html

BORSA ITALIANA
https://www.borsaitaliana.it/borsa/glossario.html

INTESA SANPAOLO