



BANCA D'ITALIA
EUROSISTEMA

PAGAMENTI ELETTRONICI E TRUFFE ONLINE

Una guida semplice per cittadini digitali





Struttura narrativa: Banca d'Italia
 Progetto grafico: Divisione Editoria e stampa della Banca d'Italia
 Coordinamento e revisione testi: Caterina Beccarini, Simone Ciccarone
 e Carlotta Rossi (Banca d'Italia)
 © Banca d'Italia, 2026
 Via Nazionale, 91 00184 Roma – Italia
 Tutti i diritti riservati.
 La collana I quaderni didattici della Banca d'Italia rientra tra le pubblicazioni
 di educazione finanziaria curate dall'Istituto. La collana è gratuita ed è
 disponibile online.
 È consentita la riproduzione a fini didattici e non commerciali, a condizione
 che venga citata la fonte.
 Per eventuali aggiornamenti consultare il sito web della Banca d'Italia
<http://www.bancaditalia.it>
 ISSN 2281 - 4094 (online)

SOMMARIO

1. Quali strumenti possiamo usare per pagare senza contante?	4
Le carte di pagamento	6
I bonifici	6
I portafogli elettronici	8
<i>Per approfondire - Come pagano gli italiani</i>	8
2. Come ci identifichiamo quando facciamo un pagamento elettronico?	10
L'autenticazione forte o autenticazione a due fattori	10
<i>Come funziona? - Le esenzioni all'autenticazione forte</i>	14
<i>Per approfondire - Il tasso di frode nei pagamenti elettronici</i>	16
3. Cos'è e come è architettata una truffa online?	18
Truffe finalizzate a far rivelare alla vittima dati riservati	20
Truffe finalizzate a far installare applicazioni malevole per carpire dati riservati	22
Truffe finalizzate a far trasferire denaro	23
<i>Come funziona? - Il furto diretto dei dati per l'autenticazione</i>	25
<i>Come funziona? - Truffe con l'intelligenza artificiale e tecniche deepfake</i>	26
4. Come possiamo proteggerci dalle truffe?	28
Piccolo vademecum per proteggersi dalle truffe online	28
<i>Istruzioni per l'uso - Una buona password, senza impazzire</i>	32
<i>Per approfondire - L'io digitale</i>	35
5. E se non si riesce a evitare una truffa?	37
Quali passi compiere se si è vittima di una truffa	37





1. QUALI STRUMENTI POSSIAMO USARE PER PAGARE SENZA CONTANTE?

Obiettivi della sezione:

- ✦ capire cosa sono i pagamenti elettronici
- ✦ riconoscere le diverse caratteristiche degli strumenti di pagamento
- ✦ conoscere le abitudini di pagamento in Italia

Negli ultimi anni, le abitudini di pagamento della popolazione sono profondamente cambiate: oggi è frequente effettuare pagamenti senza utilizzare denaro contante (monete e banconote), non solo quando si compra online ma anche quando si effettua un acquisto in negozio (cfr. [Per approfondire - Come pagano gli italiani](#)).

Quando si fanno pagamenti senza contante si usa di solito la moneta depositata nei conti correnti o, più in generale, nei conti di pagamento, che si possono immaginare come cassette virtuali, custoditi da intermediari autorizzati. Gli strumenti di pagamento alternativi al contante permettono di trasferire moneta da un conto all'altro. Richiamiamo qui in maniera sintetica i principali strumenti: carte di pagamento, bonifici e portafogli elettronici (figura 1).

Questi strumenti sono descritti con maggior dettaglio nel capitolo 3 della Guida per gli insegnanti di [Tutti per uno economia per tutti!](#).



Tutti per uno economia per tutti!

FIGURA 1

I PAGAMENTI ELETTRONICI

CARTE DI PAGAMENTO



Carte di debito

- è necessario un conto di pagamento
- l'addebito è immediato

Carte di credito

- è necessario un conto di pagamento
- l'addebito è successivo

Carte prepagate

- non è necessario un conto di pagamento
- l'addebito è immediato

BONIFICI



Bonifici ordinari

- il pagamento è completato in 1 giorno lavorativo

Bonifici istantanei

- il pagamento avviene entro 10 secondi

PORTAFOGLI ELETTRONICI



Contenitore di credenziali

- contenitore nel quale l'utente registra i propri strumenti di pagamento

Contenitore di moneta

- contenitore precaricato con moneta elettronica per effettuare transazioni con utenti dello stesso provider/circuito

Le carte di pagamento

La **carta di debito** (nota in Italia anche come Bancomat, dal nome dello storico circuito di pagamento nazionale) richiede sempre l'associazione ad un conto e consente di acquistare in negozio con un addebito immediato dell'importo: sul conto a cui la carta è collegata deve quindi essere disponibile una somma di denaro pari almeno alla spesa che si intende effettuare.

La **carta di credito**, che richiede sempre il collegamento ad un conto, consente di fare acquisti rimandando l'addebito della spesa ad un momento successivo a quello in cui si effettua il pagamento (solitamente, il mese seguente). Per questo, è possibile fare acquisti anche se al momento dell'utilizzo non si hanno fondi sufficienti sul conto: basta che i soldi ci siano nel momento previsto per l'addebito. Esiste una particolare carta di credito, la **carta di credito revolving**, che prevede la restituzione della somma non in un'unica soluzione, ad esempio nel mese successivo all'acquisto, ma a rate in più mesi. Si tratta di un servizio che ha un costo: prevede il pagamento di interessi, che possono essere elevati e che generalmente non sono richiesti nel caso di addebito in un'unica soluzione.

La **carta prepagata** non richiede il collegamento a un conto ma deve essere precaricata con fondi per poter essere utilizzata: il limite di spesa dipende anche da quanti soldi sono disponibili sulla carta. Sul mercato sono disponibili anche carte prepagate con IBAN, un codice alfanumerico che identifica in modo unico e inconfondibile ciascun conto, (cosiddette "ibanizzate"): in questo caso, oltre alle funzionalità delle carte di debito, è possibile effettuare diverse tipologie di pagamenti elettronici come ad esempio bonifici.

I bonifici

Tramite il bonifico, un individuo ordina alla propria banca di trasferire una somma dal suo conto a quello del beneficiario; se il



bonifico viene effettuato nell'Area unica dei pagamenti in euro (SEPA), il conto del beneficiario è identificato attraverso l'IBAN.

Nei **bonifici ordinari** il tempo massimo affinché la transazione sia completata è di un giorno lavorativo dopo quello di ricezione dell'ordine da parte dell'intermediario. L'operazione può essere chiusa solo nei giorni lavorativi feriali, altrimenti viene posticipata al primo giorno lavorativo utile.

Il **bonifico istantaneo**, come quello ordinario, ci consente di trasferire denaro da un conto di pagamento ad un altro, ma molto più velocemente e senza limitazioni di orario. Questo tipo di bonifico permette, infatti, di fare e ricevere pagamenti in pochi secondi 365 giorni l'anno, 7 giorni su 7, 24 ore su 24.

La velocità con cui il bonifico istantaneo viene effettuato è una gran comodità, ma richiede di prestare particolare attenzione nel verificare l'identità del destinatario del pagamento, perché proprio per le sue caratteristiche di velocità, il bonifico istantaneo non può essere revocato una volta effettuato. Per tutti i bonifici, dall'ottobre del 2025, le banche e gli altri prestatori di servizi di pagamento sono tenuti a verificare la corrispondenza tra IBAN e nome del beneficiario e questo ci mette al sicuro dagli errori ma, come vedremo più avanti, non ci mette totalmente al riparo dalle truffe (cfr. **Truffe finalizzate a far trasferire denaro** nella sezione 3). È quindi importante verificare sempre l'identità della persona o dell'azienda a cui facciamo il bonifico.

I portafogli elettronici

I **portafogli elettronici (e-wallet)** sono “contenitori” digitali che si possono creare e gestire attraverso app sul proprio smartphone. Possono essere di due tipologie: contenitore di credenziali e contenitore di moneta.

Nel caso del **contenitore di credenziali**, il cliente registra le proprie carte di pagamento. Al momento di pagare, il cliente accede al proprio *e-wallet* e sceglie quale carta utilizzare tra quelle memorizzate.

Il **contenitore di moneta**, invece, è associato ad un conto online e permette di trasferire soldi da un conto all'altro. Il pagamento è identico a un bonifico tradizionale. Quello che cambia è che l'informazione di pagamento non circola all'interno del sistema dei pagamenti a cui sono collegati tutti i diversi intermediari, ma rimane all'interno di uno specifico circuito di cui devono far parte sia chi invia e sia chi riceve il pagamento.



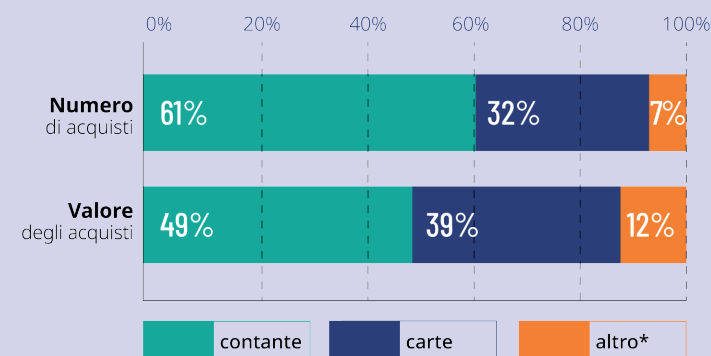
PER APPROFONDIRE COME PAGANO GLI ITALIANI

La rapida diffusione degli strumenti di pagamento elettronici sta velocemente modificando le scelte di pagamento degli individui.

Il contante rimane ancora lo strumento di pagamento più utilizzato nella maggior parte dei paesi dell'area dell'euro, tra cui l'Italia: nel nostro paese, nel 2024, 61 pagamenti su 100 nei negozi fisici erano stati effettuati con monete e banconote. Questo numero, superiore a quello medio

dell'area dell'euro pari a 52 pagamenti su 100, è significativamente inferiore a quello del 2019, quando 81 pagamenti su 100 al punto vendita avvenivano in contante. In soli 5 anni, la quota del numero di pagamenti in contante si è ridotta di 20 punti percentuali (figura A).

A. Strumenti di pagamento per gli acquisti in negozio in Italia (valore percentuale)



Note: la categoria "altro" include i pagamenti mobili, assegni bancari, bonifici, punti fedeltà, voucher, carte regalo e altri strumenti di pagamento diversi da carte e contante; dati riferiti al 2024.

Fonte: [Indagine sulle abitudini di pagamento dei consumatori dell'area dell'euro](#), BCE, 2024

Se guardiamo al valore degli acquisti, la quota dei pagamenti in contante nel 2024 era del 49 per cento in Italia e del 39 per cento nell'area dell'euro. In altri termini il contante è più usato, in proporzione, per importi più piccoli.



Indagine sulle
abitudini di
pagamento dei
consumatori
dell'area dell'euro,
BCE, 2024



2. COME CI IDENTIFICHIAMO QUANDO FACCIAMO UN PAGAMENTO ELETTRONICO?

Obiettivi della sezione:

- ✦ comprendere le modalità di identificazione quando si effettua un pagamento elettronico
- ✦ capire le caratteristiche dell'autenticazione forte
- ✦ riconoscere i casi di utilizzo e le esenzioni dell'autenticazione forte

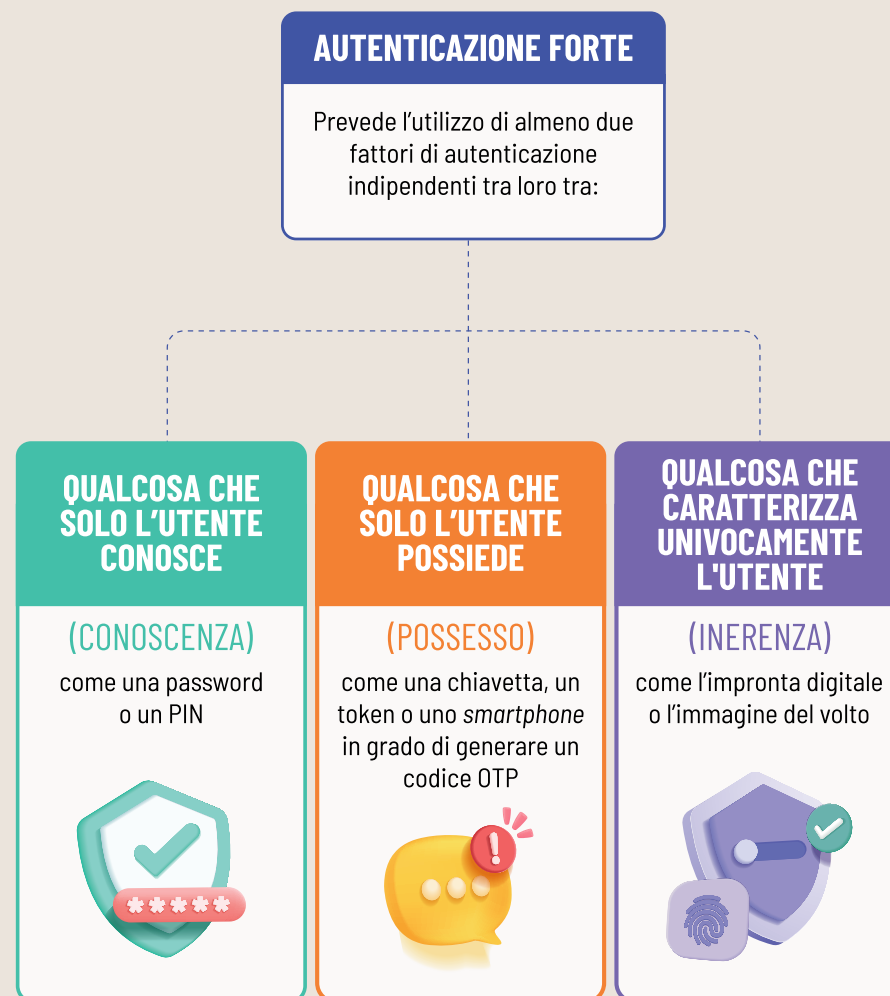
Un punto importantissimo quando si effettuano pagamenti elettronici riguarda l'identificazione di chi li effettua. Se si va in banca e si chiede di prelevare dei soldi dal proprio conto, l'impiegato verificherà che la persona che ha davanti sia effettivamente l'intestatario del conto da cui si vuole prelevare. Nel caso dei pagamenti elettronici questo non è possibile: per essere correttamente identificato, chi effettua il pagamento deve autenticarsi utilizzando credenziali che permettano di farsi riconoscere e dimostrare appunto la titolarità dello strumento che si intende utilizzare per pagare.

L'autenticazione forte o autenticazione a due fattori

Oggi, per la gran parte dei pagamenti, il meccanismo utilizzato per accertare l'identità di chi effettua il pagamento prevede l'utilizzo dell'**autenticazione forte** o a due fattori (*Strong Customer Authentication* - SCA). L'autenticazione forte è stata introdotta dalla Seconda Direttiva europea sui Servizi di Pagamento (PSD2) e prevede l'identificazione dell'utente attraverso l'uso di almeno due diversi fattori di autenticazione tra quelli indicati in figura 2.

FIGURA 2

COME CI AUTENTICHIAMO NEI PAGAMENTI ELETTRONICI?



I fattori di autenticazione sono:

- **qualcosa che solo l'utente conosce**, come una password o un PIN;
- **qualcosa che solo l'utente possiede**, come una chiavetta/*token* o uno smartphone in grado di generare un codice noto come *One Time Password* (OTP);
- **qualcosa che caratterizza univocamente l'utente**, come l'impronta digitale o il volto.

I fattori di autenticazione devono essere indipendenti tra loro; questo perché, qualora un malintenzionato entrasse in possesso di uno degli elementi di identificazione (ad esempio, della password), non potrebbe completare l'autenticazione, in quanto dovrebbe riuscire a impossessarsi anche di un ulteriore fattore.

La normativa prevede che l'intermediario fornitore dei servizi di pagamento richieda l'identificazione attraverso l'autenticazione forte ogni volta in cui l'utente:

- accede al suo conto di pagamento online;
- dispone un'operazione di pagamento elettronico (in un negozio fisico o online);
- effettua qualsiasi azione tramite un canale a distanza che può comportare un rischio di frode nei pagamenti o altri abusi (come, ad esempio, la modifica dell'utenza telefonica registrata o dei massimali periodici di effettuazione dei bonifici).

Il caso di un acquisto in negozio pagato con carta di pagamento è un buon esempio per capire come funziona l'autenticazione forte.

La carta, nel caso di pagamento in negozio, è un elemento di possesso e il PIN, che siamo tenuti a digitare per finalizzare il pagamento, è un elemento di conoscenza. Questi due elementi soddisfano le indicazioni dell'autenticazione forte quando effettuiamo un pagamento in un negozio.

A volte però il pagamento col bancomat va a buon fine anche senza l'inserimento del PIN. Perché? In caso di operazioni ben specifiche (ad esempio di basso importo e rischio limitato), gli intermediari possono, per loro scelta e con conseguente assunzione di responsabilità, non richiedere l'autenticazione forte dell'utente. Si parla, in questi casi, di esenzioni all'autenticazione forte. I casi di esenzione dall'autenticazione forte sono molto puntuali e sono riportati in **Come funziona? - Le esenzioni all'autenticazione forte**.

L'autenticazione forte ha avuto effetti positivi nel contrasto alle frodi. Uno studio della Banca d'Italia ha stimato che nel nostro paese l'autenticazione forte ha ridotto il rischio di frode del 60 per cento per i pagamenti effettuati con carta quando si acquistano beni o servizi online, e dell'80 per cento per quelli effettuati presso i negozi (cfr. M. Cologgi, [La sicurezza degli strumenti di pagamento al dettaglio: evidenze da dati di supervisione](#), Banca d'Italia 2023). In generale, a livello aggregato, nel 2023, l'incidenza delle frodi è molto bassa: basti pensare che per le carte di pagamento l'importo delle frodi è di 1,9 euro ogni 10.000 euro di pagamenti effettuati. Ma attenzione, se in aggregato questo numero è piccolo, le frodi possono avere comunque effetti non trascurabili sui singoli (cfr. **Per approfondire - Il tasso di frode nei pagamenti elettronici**).



The security of retail payment instruments: evidence from supervisory data, Banca d'Italia 2023



COME FUNZIONA?

LE ESENZIONI ALL'AUTENTICAZIONE FORTE

L'autenticazione forte, che prevede l'autenticazione attraverso due fattori indipendenti tra loro, può non essere richiesta per alcuni pagamenti. Si parla in questo caso di esenzioni che sono previste quando:

1. il pagamento è di modesto valore, al di sotto di 30 euro, e:
 - ⇒ sommato alle precedenti operazioni effettuate senza digitare il PIN non faccia superare la soglia di 100 euro.

Ad esempio, se l'utente ha già effettuato tre operazioni da 30 euro ed effettua un'operazione da 25 euro, scatterà la richiesta di SCA, perché quest'ultima operazione sommata alle precedenti in esenzione supera il valore di 100 euro;

oppure

- ⇒ non faccia superare le cinque transazioni singole consecutive senza utilizzare il PIN.

Ad esempio, se l'utente ha già effettuato 5 transazioni in esenzione per l'importo di 10 euro ciascuna, la sesta operazione di un importo anche minore di 30 euro farà scattare la richiesta di autenticazione forte perché, nonostante l'importo sia inferiore a 100 euro, si tratterebbe della sesta operazione in esenzione.

2. Il pagamento è considerato a basso rischio, di importo compreso tra 30 euro e 500 euro, nel caso in cui l'emittente della carta o l'intermediario che sta gestendo la transazione di incasso per conto del commerciante abbia un tasso di frodi pari o inferiore a determinati tassi di riferimento normativamente stabiliti.

3. Si sottoscrivono abbonamenti o pagamenti ricorrenti con valore e beneficiario fissi; l'autenticazione forte sarà richiesta solo per la prima transazione, salvo variazioni di importo.
4. Si effettua un pagamento verso un'azienda presente nella lista di "Beneficiari di fiducia"; l'autenticazione forte verrà applicata solamente al primo pagamento effettuato verso l'azienda.
5. Si effettuano operazioni *contactless* per le quali non è necessario digitare il PIN, purché il singolo pagamento non superi la soglia di 50 euro (e se i pagamenti consecutivi senza PIN, non superano il valore cumulativo di 150 euro; inoltre il numero di operazioni consecutive senza PIN non deve essere superiore a 5).

È possibile che non venga richiesta l'autenticazione forte anche nel caso di acquisti che non hanno le caratteristiche per rientrare nelle esenzioni; questo può accadere perché si effettuano transazioni con operatori che danno la possibilità di memorizzare i propri strumenti di pagamento per futuri acquisti, a fronte di un consenso iniziale. È il tipico caso di piattaforme per la vendita online o di siti di grandi società. In quei casi viene richiesta l'autenticazione forte la prima volta in cui si effettua un acquisto; successivamente, lo strumento di pagamento viene memorizzato in maniera cifrata dal commerciante e riutilizzato poi per ulteriori eventuali acquisti senza dover nuovamente inserire i dati e autenticarci con l'autenticazione forte.

Esiste, infine, la possibilità di esentare l'utente dei servizi di pagamento dall'autenticazione forte quando quest'ultimo accede al proprio conto di pagamento online per consul-

tare il saldo e le operazioni di pagamento eseguite negli ultimi 90 giorni; in questo caso, l'utente può accedere a queste informazioni con una procedura semplificata (ad esempio, utilizzando un solo fattore di autenticazione).

Queste misure, come vedremo meglio nella sezione successiva, sono un importante strumento di protezione dalle **truffe online**.



PER APPROFONDIRE
IL TASSO DI FRODE NEI PAGAMENTI ELETTRONICI

Nel nostro paese, l'incidenza delle truffe online è molto contenuta sia se guardiamo al valore delle transazioni fraudolente, e cioè dei movimenti di denaro dovuti a truffe, sia se guardiamo al numero di questi scambi.

In termini di valore, nel 2024 il valore totale delle transazioni fraudolente è stato pari a circa 4,2 miliardi di euro nell'Unione europea (UE) e a circa 278 milioni in Italia. Questo dato considera la somma del valore di tutte le transazioni fraudolente effettuate tramite bonifici, addebiti diretti, pagamenti con carta, prelievi di contante e transazioni con moneta elettronica. Il tasso di frode, cioè la quota di transazioni fraudolente sul totale delle transazioni, si attesta su livelli molto contenuti per tutti gli strumenti di pagamento sia in Italia che nella UE (tavola A). Per i bonifici, ad esempio, l'importo delle frodi in Italia è dello 0,002 per cento cioè 0,2 euro ogni 10.000 euro.

TAVOLA A
Tasso di frode sul valore dei pagamenti, per tipologia di strumento di pagamento (valore percentuale)

PAESE	BONIFICI	ADDEBITI DIRETTI	CARTE DI PAGAMENTO	PRELIEVO DI CONTANTE	TRANSAZIONI CON MONETA ELETTRONICA
Italia	0,002%	0,000%	0,021%	0,010%	0,024%
UE (*)	0,001%	0,001%	0,033%	0,010%	0,018%

Fonte: Report on payment fraud, EBA-ECB (2025), dati riferiti al 2024.
(*) Unione europea. Oltre ai paesi membri dell'Unione europea, si considerano anche Islanda, Lichtenstein e Norvegia.

Anche calcolato sulla base del numero di transazioni, il tasso di frode si attesta su valori molto bassi sia in Italia che nella UE (tavola B).

TAVOLA B
Tasso di frode sul volume dei pagamenti, per tipologia di strumento di pagamento (valore percentuale)

PAESE	BONIFICI	ADDEBITI DIRETTI	CARTE DI PAGAMENTO	PRELIEVO DI CONTANTE	TRANSAZIONI CON MONETA ELETTRONICA
Italia	0,005%	0,000%	0,012%	0,005%	0,018%
UE (*)	0,002%	0,013%	0,015%	0,005%	0,011%

Fonte: Report on payment fraud, EBA-ECB (2025), dati riferiti al 2024.
(*) Oltre ai paesi membri dell'Unione europea, si considerano anche i dati di Islanda, Lichtenstein e Norvegia.

Nonostante questi dati possano sembrare incoraggianti, è comunque importante mantenere alta l'attenzione per evitare di incappare in eventi fraudolenti.



3. COS'È E COME È ARCHITETTATA UNA TRUFFA ONLINE?

Obiettivi della sezione:

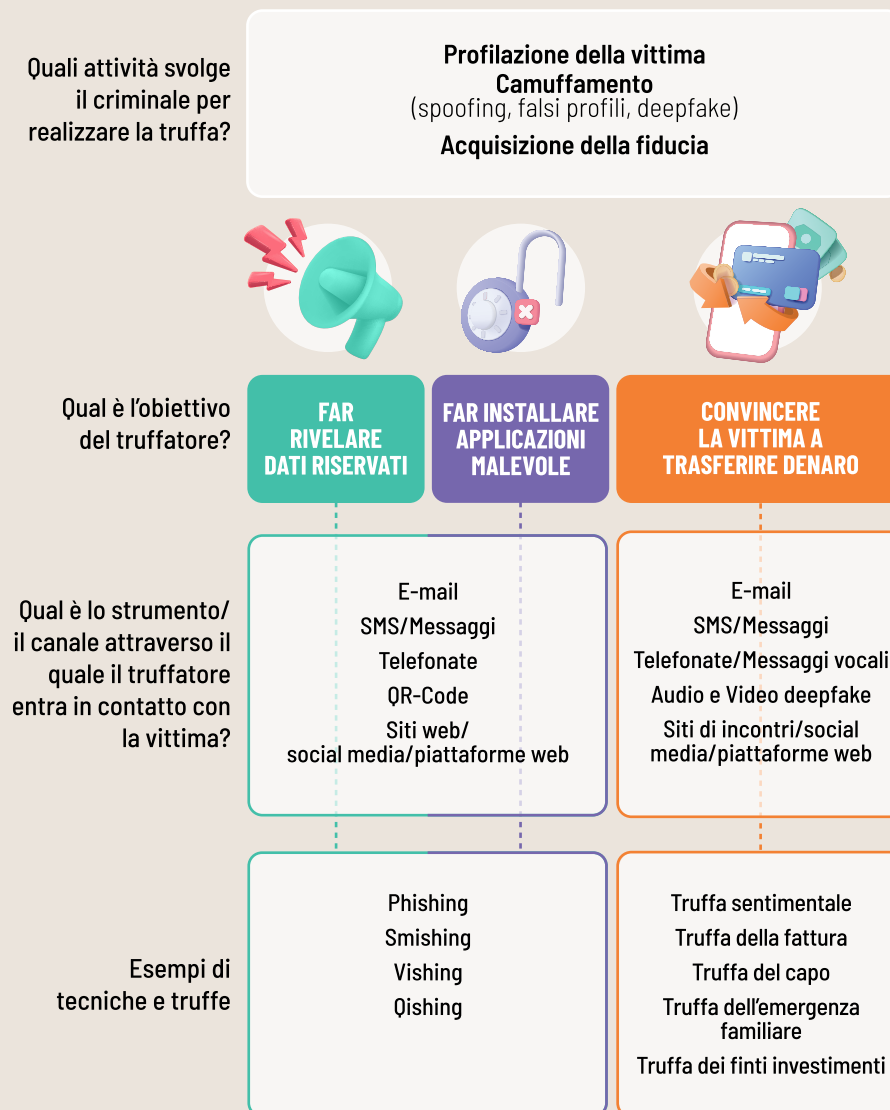
- ✦ comprendere cosa sono le truffe
- ✦ conoscere le caratteristiche delle principali truffe
- ✦ riconoscere i segnali di una possibile truffa

Secondo l'articolo 640 del codice penale, la truffa è un reato che consiste nell'ingannare una persona attraverso artifici o raggiri, inducendola in errore al fine di ottenere un ingiusto profitto a danno della vittima.

Questo comportamento fraudolento può comportare pene variabili, che vanno dalla multa alla reclusione. Per rafforzare il contrasto a queste tipologie di crimini effettuati online e aumentare la sicurezza degli utenti, sono state introdotte una serie di modifiche al codice penale con la L. 90/2024 (Disposizioni in materia di rafforzamento della sicurezza cibernetica nazionale e di reati informatici). In seguito alla modifica legislativa, commettere una truffa a distanza attraverso strumenti informatici o telematici configura un'aggravante del reato che determina l'inasprimento della pena.

In ambito finanziario, le truffe online sono costruite per ingannare la vittima e indurla a compiere determinate azioni attraverso specifiche tecniche. Ricondurre le truffe a una tassonomia precisa non è affatto semplice perché i criminali sviluppano truffe sempre più complesse, che possono avere più di una finalità e combinano contemporaneamente diversi strumenti e tecniche di realizzazione. Con questi limiti, in figura 3 proponiamo un quadro di sintesi delle principali truffe articolato in base agli obiettivi di chi attua la truffa e le tecniche utilizzate per realizzarla.

FIGURA 3 LE TRUFFE ONLINE



Partendo dagli obiettivi, possiamo individuare tre grandi tipologie di truffe:

1. **truffe finalizzate a far rivelare alla vittima i dati riservati** come le proprie credenziali di accesso all'home-banking, dati delle carte di pagamento o i codici OTP;
2. **truffe finalizzate a far installare applicazioni malevole per trafugare dati riservati, come ad esempio le credenziali per accedere al conto bancario, mediante link**, allegati o direttamente dai *mobile store*;
3. **truffe il cui obiettivo è convincere la vittima a trasferire denaro** incautamente a un soggetto terzo.

Truffe finalizzate a far rivelare alla vittima dati riservati

Per realizzare queste truffe i cyber criminali usano differenti canali per contattare la vittima, a ciascuno dei quali corrisponde una specifica tipologia di truffa: **phishing** (via e-mail), **smishing** (attraverso messaggi via sms o altri sistemi di messaggistica istantanea), **vishing** (mediante telefonate), **qishing** (attraverso QR code).

Queste truffe spesso sfruttano vulnerabilità psicologiche degli individui, come il timore di vedere bloccato l'accesso al proprio conto bancario oppure il desiderio di ricevere un premio in denaro o vantaggi esclusivi. Sono anche dette **tecniche di ingegneria sociale** (*social engineering*): come nell'ingegneria si usano materiali per costruire edifici, così nell'ingegneria sociale si usano le emozioni, come l'ansia o il timore, per creare inganni e indurre le persone a compiere le azioni volute.

Le tecniche di ingegneria sociale si intrecciano poi con **tecniche di camuffamento**, come lo *spoofing*, tra cui l'alterazione dell'indirizzo e del nome del mittente di un'e-mail, la falsificazione del nominativo del mittente che appare alla ricezione di un sms o tramite un'app di messaggistica istantanea, la falsificazione del

numero di telefono dal quale sembra provenire una telefonata. Con lo *spoofing* il truffatore mira a far credere all'utente di essere stato contattato da una controparte con cui ha abitualmente contatti, ad esempio la sua banca. I cyber criminali possono predisporre siti web molto simili nel nome e/o nell'aspetto a quelli reali (c.d. *typo-squatting*), ad esempio quello di una banca.

Ecco due esempi.

Il Phishing

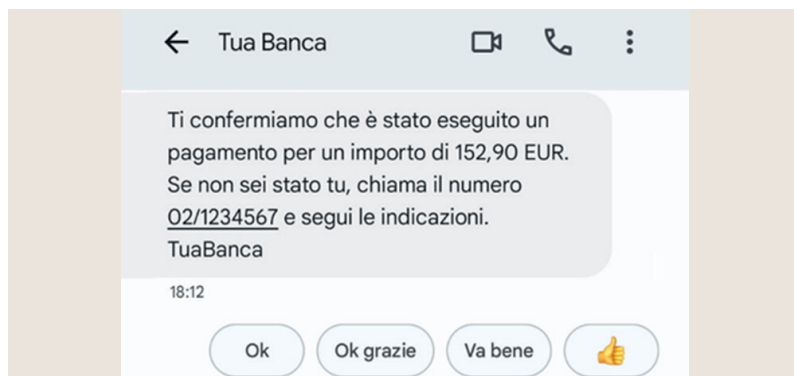


Questo è un esempio di *phishing*; il truffatore invia un'e-mail con cui cerca di ottenere dalla vittima dati riservati.

L'e-mail contiene elementi tipici delle tecniche di ingegneria sociale: la minaccia del blocco della carta e una scadenza ravvicinata entro cui questo fatto avverrà puntano a suscitare preoccupazione ed ansia in chi la riceve e sollecitano un'azione immediata.

Inoltre sono presenti elementi di camuffamento: l'indirizzo del sito web contenuto nell'e-mail non è quello corretto anche se simile a quello della banca: se andassimo con il mouse sul link apparirebbe l'indirizzo **www.tuabanca.com.tk** diverso da quello dell'intermediario **www.tuabanca.net**.

Lo Smishing



Questo è un esempio di *smishing*; il truffatore invia un sms con cui cerca di far chiamare dalla vittima la sua presunta banca, attivando successivamente meccanismi per ottenere dati riservati.

In questo caso il numero di telefono non è quello della “presunta” banca ma è sotto il controllo dei truffatori.

I criminali possono mettere in atto anche altri meccanismi, con tecniche che non richiedono un coinvolgimento diretto della vittima, per rubarne le credenziali di autenticazione (cfr. [Come funziona? - Il furto diretto dei dati per l'autenticazione](#)).

Truffe finalizzate a far installare applicazioni malevole per carpire dati riservati

I cyber criminali possono inviare, via e-mail o sistemi di messaggistica istantanea, allegati o link a contenuti malevoli che hanno l'obiettivo di infettare lo smartphone o il computer della vittima con un **malware sviluppato per carpire i dati riservati presenti nel dispositivo**. I *malware* (parola composta da “malicious” e “software”) sono programmi progettati per danneggiare i dispositivi degli utenti, ottenere accessi non autorizzati e rubare/compromettere i dati: un *malware* può permettere a un cyber-

criminale di ottenere le password e i PIN memorizzati nel nostro computer o nel nostro smartphone, oppure di intercettarli mentre vengono digitati dall'utente.

Truffe finalizzate a far trasferire denaro

Questa categoria di truffe comprende quelle dirette a indurre la vittima a effettuare pagamenti in favore del truffatore. Anche in questa categoria di truffe la vittima può essere contattata attraverso diversi canali di comunicazione utilizzando tecniche di ingegneria sociale: i messaggi possono contenere riferimenti ai gusti o alle preferenze della potenziale vittima, carpite dai truffatori in base alle tracce digitali lasciate nel web (cfr. [Per approfondire - L'io digitale](#) nella sezione 4).

Un esempio è la **truffa sentimentale** (*romance scam*). I malintenzionati prendono di mira le vittime sui siti di incontri online, sui social media o attraverso e-mail, dichiarando di provare forti sentimenti nei loro confronti e cercando di avviare una relazione a distanza. I criminali lavorano pazientemente per ottenere la fiducia delle vittime per poi chiedere denaro, regali o anche i dati della carta di credito.

Un altro esempio è la **truffa dell'emergenza familiare** (*family emergency scam*). I criminali si spacciano per un familiare in difficoltà e, tramite telefonate o messaggi, chiedono con urgenza un trasferimento di denaro per risolvere un presunto problema (incidenti, arresti, emergenze mediche). L'obiettivo è sfruttare l'emotività della vittima per indurla a pagare senza verificare la veridicità della richiesta. Attraverso l'utilizzo di strumenti di intelligenza artificiale, i criminali sono in grado di manipolare o generare artificialmente la voce (c.d. *deepfake*) del presunto familiare in difficoltà e veicolare la truffa attraverso telefonate o messaggi vocali (cfr. [Come funziona? - Truffe con l'intelligenza artificiale e tecniche deepfake](#)). Altre truffe riconducibili a questa categoria sono la [truffa della fattura](#) e la [truffa del capo](#).



La truffa della fattura



La truffa del capo



La web serie
I Navigati

PER PARLARNE IN CLASSE



Le truffe di cui abbiamo parlato in questa sezione e i meccanismi alla base della loro realizzazione sono descritti nella web serie I Navigati realizzata dal CERTFin.

CERTFin è un'iniziativa cooperativa pubblico-privata, di cui la Banca d'Italia fa parte, finalizzata a innalzare la capacità di gestione del rischio informatico degli operatori finanziari e la resilienza cibernetica del sistema finanziario italiano. La serie comprende brevi video basati sulle storie di una famiglia che si trova a fare i conti con le insidie del web; sono video adatti a essere utilizzati anche con un pubblico di ragazze e ragazzi. Cerca I Navigati anche su Instagram, Facebook e YouTube.



CERTFin



COME FUNZIONA?

IL FURTO DIRETTO DEI DATI PER L'AUTENTICAZIONE

Abbiamo appena visto che i cyber criminali possono entrare in possesso delle nostre credenziali (username, password, PIN, OTP, etc.) facendo in modo che siamo noi stessi a consegnargliele; ma possono entrarne in possesso anche con tecniche che non richiedono un nostro coinvolgimento diretto. Come?

- **recuperandole:** le informazioni personali presenti sui social, come la data di nascita, il nome di fratelli e sorelle o del gruppo musicale preferito, possono essere utilizzate per indovinare una password o un PIN. A volte l'analisi di quello che pubblichiamo sui social e più in generale le tracce che lasciamo nel web (cfr. **Per approfondire - L'Io digitale** nella sezione 4) forniscono un grande aiuto ai truffatori;
- **conducendo attacchi a "forza bruta":** i cyber criminali possono mettere in atto meccanismi per eseguire automaticamente milioni di tentativi provando ogni possibile combinazione di caratteri fino a individuare la password o il PIN ... è solo questione di tempo se le credenziali non sono robuste!
- **conducendo "attacchi a dizionario":** i criminali possono mettere in atto meccanismi per tentare in sequenza ciascuna delle parole di senso compiuto elencate in un dizionario fino a trovare quella che corrisponde alla password corretta;
- **mediante password spraying:** letteralmente "spruzzatura delle password", si tratta di una variante dell'at-

tacco a forza bruta in cui un insieme limitato di password comuni vengono tentate per accedere a un gran numero di account;

- **spiando:** un malintenzionato potrebbe osservare la vittima mentre digita la password o il PIN;
- **intercettandole:** i dati di una carta di pagamento possono essere intercettati manomettendo il terminale ATM o POS dal quale si effettua un'operazione (*skimming*) oppure compromettendo un sito di e-commerce legittimo (*e-skimming*);
- **acquistandole nel dark web:** un criminale può comprare nel "mercato nero" del *dark web* archivi digitali contenenti credenziali o dati delle carte di pagamento di utenti, rubati dai loro dispositivi oppure dai server che erogano servizi online.



COME FUNZIONA?

TRUFFE CON L'INTELLIGENZA ARTIFICIALE E TECNICHE DEEPFAKE

Con il termine deepfake si intende la manipolazione o la generazione artificiale di audio, video o altre forme di contenuti digitali attraverso l'applicazione di tecniche di intelligenza artificiale generativa. In particolare, partendo da contenuti audio/video originali, è possibile replicare e/o modificare sinteticamente l'immagine, il video o la voce di una persona per creare contenuti che appaiono estremamente realistici. Ad esempio, come abbiamo visto nel-

la **truffa dell'emergenza familiare**, è possibile generare falsi messaggi vocali con una voce identica a quella di un parente.

Circolano inoltre nel web video realizzati con tecniche deepfake che, in maniera artefatta, riproducono il volto e la voce di esponenti governativi e di istituzioni finanziarie e altri personaggi noti al fine di veicolare e rendere credibili messaggi non veritieri con intenti fraudolenti, ad esempio per convincere il pubblico ad acquistare determinati strumenti di investimento (c.d. truffa dei finti investimenti).

Inizialmente il costo della tecnologia necessaria per realizzare un contenuto deepfake era piuttosto elevato e ciò ha tenuto per molto tempo circoscritti i suoi ambiti di applicazione. Oggi non è più così: gli strumenti che consentono la manipolazione video (e audio) sono economici e di facile utilizzo. Proteggersi da questo tipo di minacce non è semplice: cosa si può fare per affrontare una manipolazione della realtà così pericolosa da rendere credibile, potenzialmente, qualsiasi cosa?

Il primo elemento di difesa è proprio la consapevolezza di quanto sia importante selezionare le fonti di informazione in base al loro grado di attendibilità. Quando guardiamo un video, anche se sembra perfettamente realistico, dobbiamo tenere presente che potrebbe non essere autentico. È sempre buona pratica verificarne le informazioni attraverso altre fonti affidabili (ad esempio i quotidiani o i siti ufficiali delle istituzioni). Inoltre, davanti a un caso di sospetto deepfake sarà importante non dare seguito alle eventuali richieste avanzate nei video ed evitare di condividerlo per non contribuire ad aumentarne la diffusione.



4. COME POSSIAMO PROTEGGERCI DALLE TRUFFE?

Obiettivi della sezione:

- ✦ comprendere cosa fare per proteggersi dalle truffe
- ✦ spiegare le regole di buona condotta da mettere in pratica

Le truffe sono in continua evoluzione ma alcune regole di buona condotta possono aiutare a non cadere in trappola. Qui di seguito le principali regole da tenere a mente (figura 4).

Piccolo vademecum per proteggersi dalle truffe online

1. Verificare sempre l'identità di chi ci contatta

I criminali spesso si fingono soggetti di cui pensiamo di poter fidare, un familiare, un amico, la nostra banca; è importante verificare la reale identità di chi ci contatta controllando in modo indipendente rispetto alla comunicazione ricevuta (anche mediante il sito dell'Agenzia delle Entrate).

- ✦ **Attenzione:** a volte per un occhio non esperto è molto difficile distinguere indirizzi veri da indirizzi falsi; nel caso di comunicazioni da presunti intermediari è, quindi, sempre opportuno non cliccare sui link contenuti nel messaggio e utilizzare, invece, i link salvati in precedenza nei segnalibri e/o tra i siti preferiti per accedere ai siti legittimi.

2. Attenzione al linguaggio e ai toni

È importante prestare attenzione ai toni delle comunicazioni e a errori grammaticali e di sintassi di e-mail, messaggi e

telefonate. Molte truffe sono realizzate attraverso e-mail e messaggi costruiti con tecniche di ingegneria sociale: messaggi che parlano di grandi vincite, di vantaggi inattesi ma anche di pericoli o di danni probabili, dai toni urgenti e perentori, devono essere letti con senso critico e indurci a fare verifiche prima di rispondere. In particolare, è bene essere molto cauti nei confronti di avvisi di eventuali anomalie da parte della presunta banca, richieste di aggiornamenti necessari, segnalazioni di operazioni anomale realizzate da terzi. Errori di grammatica o di sintassi sono spesso presenti in messaggi di truffatori. Alcuni messaggi possono anche risultare particolarmente verosimili perché contengono dettagli personali della vittima, di amici o familiari come ad esempio la data di una ricorrenza o il riferimento a una attività appena svolta. In questi casi è bene ricordare che i criminali possono sfruttare i dati che ciascuno di noi condivide in rete, ad esempio attraverso l'uso dei social network, per costruire truffe altamente personalizzate, rendendole molto credibili e difficili da riconoscere (cfr. [Per approfondire - L'Io digitale](#)).

3. Proteggere i propri dispositivi

Mantenere in sicurezza il PC e lo smartphone è essenziale per prevenire le truffe. È quindi importante installare gli aggiornamenti di sicurezza dei dispositivi quando vengono resi disponibili. Inoltre è importante non installare mai software ottenuti mediante link presenti in e-mail o messaggi sospetti, installare app solo dagli store ufficiali e verificare l'attendibilità di qualsiasi app prima di installarla.

4. Controllare frequentemente i movimenti bancari

È buona regola tenere sotto controllo i pagamenti, verificando spesso la lista dei movimenti del conto o della carta. È importante individuare il prima possibile eventuali operazioni non autorizzate o non correttamente eseguite, anche adot-

tando servizi di notifica automatica, come gli sms alert, che la banca è tenuta a fornire, salvo esplicito rifiuto dell'utente di avvalersene. L'sms alert informa di ogni pagamento effettuato, rendendo, quindi, più semplice segnalare con tempestività eventuali pagamenti non autorizzati.

5. Usare con attenzione gli strumenti di pagamento digitali

È buona regola utilizzare gli strumenti di pagamento digitali secondo quanto previsto dal contratto e proteggere le nostre credenziali con diligenza. Abilitare, dove possibile, l'autenticazione a più fattori è senz'altro un'importante misura di protezione, ma questo non sempre è possibile e, comunque, molto spesso utilizziamo ancora, come primo fattore di autenticazione, PIN o password per accedere ai servizi o effettuare acquisti online. Per questo motivo, è importante non conservare il PIN delle carte di pagamento nello stesso posto in cui sono custodite le carte: sarebbe come lasciare le chiavi di casa nella serratura. Inoltre, è importante utilizzare una buona password, robusta, ma anche "facile" da ricordare (cfr. **Istruzioni per l'uso - Una buona password, senza impazzire**).

6. Non inserire mai le proprie credenziali in risposta a un messaggio o una telefonata di una presunta banca

Una banca non contatterà mai il cliente con e-mail, messaggi o telefonate chiedendo dati relativi a carte di pagamento, credenziali di accesso all'home banking o altre informazioni personali.

Per connettersi al sito della propria banca è fondamentale scrivere direttamente l'indirizzo nella barra di navigazione oppure utilizzare i link salvati in precedenza nei segnalibri e/o tra i siti preferiti e non cliccare su link presenti in e-mail o altri messaggi, in quanto questi potrebbero condurre a un sito contraffatto, molto simile all'originale.

FIGURA 4

VADEMECUM PER PROTEGGERSI DALLE TRUFFE ONLINE



1. Verifica sempre l'identità di chi ti contatta



2. Fai attenzione al linguaggio e ai toni dei messaggi



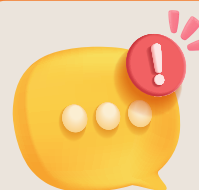
3. Proteggi i tuoi dispositivi



4. Controlla frequentemente i movimenti bancari

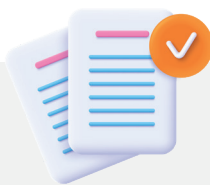


5. Usa con attenzione gli strumenti di pagamento elettronici



La tua banca non ti contatterà mai chiedendo dati relativi a carte di pagamento, credenziali di accesso all'home banking o altre informazioni personali.

RICORDA!



ISTRUZIONI PER L'USO

UNA BUONA PASSWORD, SENZA IMPAZZIRE

Una buona password deve essere **robusta**, ma deve anche essere nostra alleata e, cioè, **facile per noi da ricordare**.

Quali sono le caratteristiche di una password robusta?

- ✓ **È lunga:** la lunghezza è il fattore più importante che determina la robustezza di una password; più una password è lunga, più è difficile che possa essere indovinata in un lasso di tempo ragionevole;
- ✓ **include tanti tipi di caratteri:** lettere minuscole, maiuscole, numeri e simboli (punteggiatura e altri caratteri);
- ✓ **non parla di noi** (ma neanche della nostra famiglia): la password non dovrebbe mai contenere informazioni personali; generalmente siamo portati a creare password basate su informazioni che ci riguardano perché sono facili da ricordare, ma sono anche facili per chiunque da reperire online, ad esempio sui nostri profili social (se ho scelto la data di nascita del mio cane o gatto come password e poi pubblico su Facebook un messaggio di auguri per il suo compleanno, sto fornendo elementi per indovinare la mia password);
- ✓ **viene usata per un solo scopo:** è importante evitare di riciclare vecchie password e differenziare le password di lavoro da quelle personali evitando di usare la stessa password per tutti i nostri account; altrimenti, se qualcuno dovesse scoprirla, otterrebbe l'accesso a tutti i servizi sui quali l'abbiamo utilizzata e alle informazioni in essi contenute;
- ✓ **non è già stata "rubata":** una password robusta non deve comparire negli elenchi di password rubate. Esi-

stono, purtroppo, numerosi casi di violazione dei dati personali che hanno comportato l'esposizione online di grandi archivi di password rubate, liberamente accessibili a chiunque. Una password che sia stata compromessa in tale modo non è più sicura: non deve essere utilizzata perché è entrata a far parte di quei "dizionari" che i cyber criminali utilizzeranno per nuovi attacchi. Questi elenchi, così preziosi per i criminali informatici, possono altresì costituire un'ottima arma di difesa per noi, in quanto consentono agli strumenti di protezione installati sui nostri dispositivi di notificarci se le nostre password, già in uso oppure quelle che vorremmo impostare, sono presenti in essi.

Abbiamo detto che una buona password deve essere robusta ma anche facile da ricordare. Ognuno di noi gestisce talmente tante password che ricordarle tutte è davvero uno sforzo improbo: si è calcolato che ciascuno di noi debba ricordare all'incirca 100 password/PIN/dati di sicurezza. L'affanno generato dalla difficoltà di gestire questi dati ha portato all'identificazione di una particolare patologia: la "*password fatigue*" (affanno da password) che colpisce sempre più spesso i cittadini digitali. Questo affanno porta, purtroppo, ad attuare comportamenti poco sicuri: troppo spesso le password vengono considerate una costrizione, un ostacolo al rapido accesso al servizio; così pensiamo di aggirare il problema non utilizzandole o usando password deboli, la cui capacità di tutelare la nostra identità digitale è del tutto insufficiente. Scegliere password semplici o utilizzare la stessa password su più account rende la vita molto più semplice ai cyber criminali.

Ma come possiamo costruire una password robusta che sia anche facile da ricordare/ricchiama-re?

- **Usando passphrase:** cioè una password lunga almeno 15 caratteri, con numeri e simboli di punteggiatura, e composta da più parole che formano una piccola frase, non necessariamente di senso compiuto, ma semplice da ricordare (ispiriamoci al verso di una canzone o di una poesia; prendiamo spunto da una citazione memorabile di un film o di un libro; inventiamo una divertente filastrocca priva di senso; scegliamo le iniziali delle parole di una frase lunga che ricordiamo facilmente);
- **usando il password manager:** è un software nato proprio per ricordare al nostro posto tutte le password che utilizziamo, persino le più complesse o quelle che usiamo più raramente. Ma il password manager fa qualcosa di più che ricordare, è anche in grado di proteggere le nostre password, conservando in un unico luogo tutte le nostre credenziali. Per accedere al nostro password manager bisognerà digitare una password principale, la chiave di accesso a tutte le password contenute e memorizzate nel password manager. Non serve, quindi, sottolineare quanto sia importante scegliere una password principale, che sia per noi indimenticabile e per i cyber criminali irraggiungibile. I password manager più evoluti ci aiutano, suggerendo password complesse e uniche, oppure segnalando quando queste siano deboli o già presenti in elenchi di password rubate.

PER APPROFONDIRE L'IO DIGITALE



Ogni volta che navighiamo in Internet, comunichiamo attraverso i social network, pubblichiamo recensioni, utilizziamo il navigatore del nostro smartphone e facciamo acquisti online, lasciamo delle tracce digitali. L'insieme delle tracce che lasciamo online svolgendo queste tipologie di attività costituisce il **nostro Io digitale o digital footprint**.

Si parla di Io digitale attivo quando è l'utente che condivide deliberatamente le informazioni (ad esempio la recensione di un film); si parla invece di Io digitale passivo quando le tracce digitali (come l'indirizzo IP e le caratteristiche del dispositivo utilizzato e molto altro) sono diffuse senza che l'utente ne sia consapevole.

I dati diffusi in rete in vario modo sono davvero tanti e questa enorme quantità di dati è una merce preziosa nel web. Le tracce che lasciamo nel web vengono infatti sfruttate dalle aziende per costruire un identikit dei potenziali clienti e rivolgere a essi messaggi promozionali "su misu-

ra”, molto vicini alle abitudini e alle preferenze dei singoli. Questa attività si chiama **profilazione o profiling** e si basa su algoritmi che analizzano tutti i dati raccolti durante le attività compiute dagli utenti nella navigazione: quali siti sono visitati, quali ricerche sono effettuate, quali pagine sono condivise con altri, quali notizie attraggono di più, per quanto tempo vengono visualizzate, quali azioni conseguenti alla navigazione sono compiute, con quali dispositivi, etc.

Purtroppo, le informazioni che lasciamo navigando nel web potrebbero anche essere utilizzate per scopi malevoli con conseguenze dirette su di noi, sulla nostra famiglia o sul nostro lavoro. **I cyber criminali sfruttano infatti tali informazioni** per organizzare truffe ai danni nostri o delle persone a noi vicine come nel caso della truffa dell'emergenza familiare.



5. E SE NON SI RIESCE A EVITARE UNA TRUFFA?

Obiettivi della sezione:

- ✦ comprendere quali sono le tutele a disposizione
- ✦ spiegare come funzionano un ricorso all'ABF e un esposto alla Banca d'Italia
- ✦ riconoscere diritti e doveri dell'intermediario e del cliente
- ✦ fornire i riferimenti sui canali di denuncia e di contrasto dei crimini online previsti dalle forze dell'ordine

Quali passi compiere se si è vittima di una truffa

Quando si è vittima di truffa finanziaria, la prima cosa da fare è sempre quella di rivolgersi alla propria banca o intermediario per disconoscere il pagamento e chiedere la restituzione delle somme sottratte. Nel caso in cui i truffatori abbiano compromesso una carta di pagamento, bisogna procedere al blocco della carta. A volte i clienti vengono risarciti già in questa fase (entro la giornata successiva). Nel caso in cui si ritenga che il comportamento della banca o dell'intermediario non sia stato corretto, si può fare un reclamo. La legge prevede che per **reclami** relativi ai pagamenti il tempo massimo di risposta delle banche sia più breve rispetto a quello degli altri prodotti bancari, ovvero di soli 15 giorni.

Se non si è soddisfatti della risposta della banca, o in mancanza di risposta, si può presentare un **ricorso all'Arbitro Bancario Finanziario (ABF)**, un sistema di risoluzione stragiudiziale delle controversie. Il ricorso si presenta tramite una piattaforma online, ha un costo di 20 euro, che vengono restituiti in caso di esito favorevole

e non serve l'assistenza di un avvocato. Il ricorso all'Arbitro è uno strumento di tutela molto efficace nel caso in cui qualcosa vada storto, sebbene gli intermediari non siano vincolati al rispetto delle decisioni dell'Arbitro. Il ricorso può essere particolarmente utile quando la controversia ha ad oggetto importi contenuti, per i quali i costi e i tempi dell'accesso alla giustizia ordinaria potrebbero risultare eccessivi. I tempi di risoluzione sono estremamente rapidi.

Chi intende segnalare un comportamento irregolare o scorretto da parte di una banca o altra società finanziaria può presentare anche un **esposto alla Banca d'Italia**. Quando riceve un esposto, la Banca d'Italia sollecita l'intermediario a prendere in esame quanto segnalato e a rispondere al cliente, agevolando così il dialogo tra le parti. La Banca d'Italia non interviene con una propria decisione nel merito dei rapporti contrattuali tra intermediario e cliente, come ad esempio può fare l'ABF.

Ma si ha sempre diritto a riavere indietro i soldi?

Dipende. In linea di principio, se il cliente non ha agito in modo fraudolento e si è comportato in modo diligente, ha diritto a essere rimborsato. È importante, perciò, avere ben chiara la ripartizione dei diritti e degli obblighi tra banca e clienti.

In generale il diritto al rimborso è garantito:

- in caso di operazioni per le quali non ci sia stata l'autenticazione forte;
- per le operazioni per le quali era prevista l'autenticazione forte ma è stata accertata l'assenza di dolo o colpa grave da parte del cliente.

Proprio per evitare di incorrere in comportamenti riconducibili a dolo o colpa grave, i clienti sono tenuti a usare gli strumenti e i servizi di pagamento in modo attento, rispettando le previsioni del contratto, adottando misure idonee ad assicurare la segretezza delle proprie credenziali e comunicando tempestivamente

alla banca l'esecuzione di operazioni non autorizzate. Un cliente che rispetta queste regole si è comportato in maniera corretta e, in caso di truffa, ha di norma diritto a ricevere un rimborso. Invece, se il cliente cade in truffe molto note o facilmente riconoscibili, dimostra un comportamento negligente e potrebbe perdere il diritto al rimborso. Per questo motivo è importante che il cliente sia vigile e informato sulle tecniche utilizzate dai truffatori per evitare di cadere vittima di truffe.

Inoltre, quando si subisce una truffa o un tentativo di truffa, è bene tenere a mente che, per tutelare le persone e per contrastare queste forme di reato, è possibile presentare una denuncia alla Polizia Postale, sia presso le sedi della stessa, sia attraverso gli altri canali messi a disposizione. Per maggiori informazioni si può visitare [la sezione dedicata](#) alle segnalazioni sul sito della Polizia Postale.

Per saperne di più sulla tutela del cliente bancario è inoltre possibile consultare il sito [L'economia per tutti](#).



Sito della Polizia Postale



L'economia per tutti

