Menu

Economia e finanza riguardano tutti

Secondo **OCSE** (Organizzazione per la Cooperazione e lo Sviluppo Economico) la **Finacial Literacy**, ovvero **la cultura della gestione del denaro**, è una competenza utile a:

comprendere **concetti e rischi** finanziari,

prendere **decisioni informate** per risparmiare o investire,

migliorare il proprio **benessere finanziario** (e quello della propria famiglia odierna e futura),

consentire la partecipazione alla **vita economica**.

Un’identità… bancaria

Anche in banca, per gestire il denaro, avere prestiti, accendere mutui, ecc. bisogna prima di tutto **avere una propria identità**:

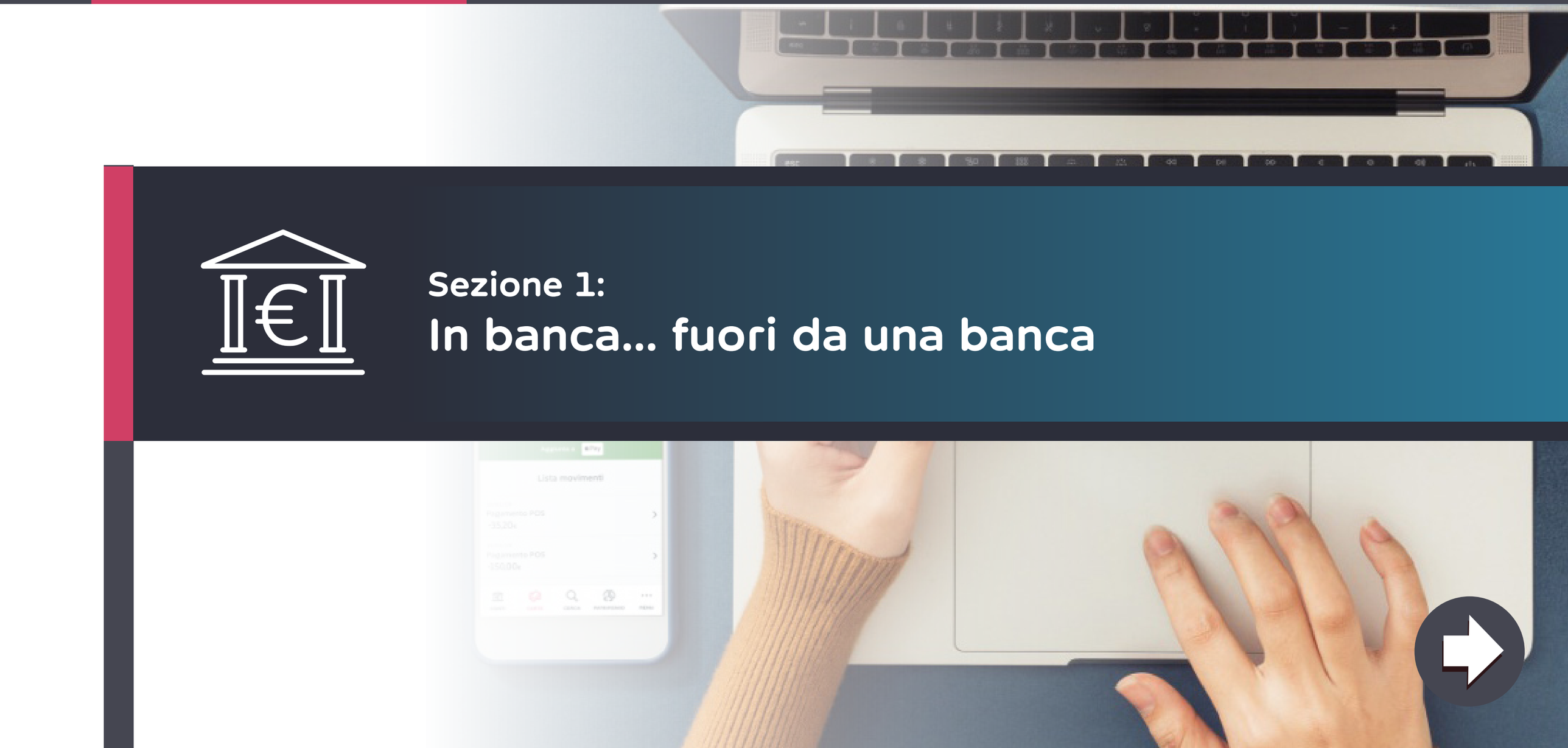
ne abbiamo una **fiscale** (Codice Fiscale),
una **sanitaria** (tessera sanitaria),
una **anagrafica** (carta di identità e passaporto),
ed ora anche una **digitale** (Spid).

Fino a poco tempo fa, l’identità bancaria era il numero del nostro conto corrente, e si gestiva andando in filiale:
oggi anche questa identità diventa più… smart!

Educazione finanziaria ed educazione digitale

Finacial Literacy e competenze digitali, sono sempre più collegate: oggi **l'identità bancaria è anche digitale.**

Secondo l'indagine Global FinLit Survey (2018) sugli over 15 in 140 paesi del mondo, **il 63% dei cittadini italiani non possiede conoscenze finanziarie di base**, mentre OCSE sottolinea come solo **il 21% delle persone tra i 16 e i 65 anni abbia un buon livello di alfabetizzazione informatica.**



Sezione 1:
In banca... fuori da una banca

Nel **2021** il 45% degli italiani ha drasticamente ridotto o cessato il rapporto fisico con la banca: per la fascia d'età **18-29 anni la percentuale sale al 50%.**

Il 68% degli italiani che possiedono un conto bancario preferisce il **mobile banking** (da smartphone) rispetto ad altri canali di contatto con la loro banca. (fonte: Osservatorio Hybrid Lifestyle di Nomisma).

La vostra famiglia va ancora in filiale? Quanto spesso?

MESCOLIAMO LE IDEE

Che cos'è un pagamento elettronico: dal bonifico al contactless

Un pagamento elettronico è una transazione avviata ed elaborata esclusivamente con mezzi elettronici, **senza denaro contante, assegni o assegni circolari.**

Il pagamento elettronico **più "tradizionale" è il bonifico bancario**, mentre una delle forme più **"avanzate"** è il cosiddetto **pagamento "contactless"**, senza alcun contatto fra strumento di pagamento e dispositivo terminale del ricevente.

App di pagamento

Paypal, Satispay, Bancomat Pay, Apple e Google Pay
... Come funzionano?

Grazie a queste app, smartphone e wearable (orologi smart) si trasformano in carte **“contactless”** nei negozi fisici e, grazie ad autenticazioni sicure, negli e-commerce.

Rapidità, igiene e sicurezza,
ma anche interessanti servizi aggiuntivi,
come **protezione sugli acquisti**
o rimborso delle **spese di reso**:
questi sono altri punti di forza di queste app.

Smart payment

I pagamenti con smartphone o wearable non sono smart
solo perché effettuati con questo tipo di dispositivi:
**sapete in quanto tempo ci accorgiamo di aver smarrito
il telefono mediamente?**

15 minuti, a fronte di 2 ore per lo smarrimento di un portafoglio;
se a questo sommiamo le funzionalità di riconoscimento
e blocco di cui è dotato uno smartphone,
sarà facilmente comprensibile capire
quanto gli smart payment siano più sicuri.

Pagare “peer-to-peer”

Gli smart payment funzionano sulla base di tecnologie di scambio fra utenti, le quali consentono una interazione **“contactless”** tra il mezzo di pagamento ed il dispositivo di ricezione dello stesso, sfruttando protocolli di **comunicazione in radiofrequenza o crittografie grafiche.**

ANDIAMO AL PUNTO

ANDIAMO AL PUNTO

Grazie alla tecnologia **NFC “near field communication”**, ovvero “comunicazione a stretto raggio”, si avvicina lo smartphone (o l’orologio) al lettore di carte POS (Point Of Sale) e si effettua il pagamento. Anche in questo caso la sicurezza è massima: i due dispositivi devono essere entrambi **sbloccati, attivati e ad una distanza massima fra loro di 4cm.**

In alcuni casi, potrebbe invece essere necessario scansionare un **codice a risposta rapida QR-code**: un quadrato grafico in grado di contenere molte più informazioni di un tradizionale codice a barre, fra le quali la disposizione di pagamento.

Sezione 2:

Occhio al portafoglio... digitale

Secondo l'indagine OCSE-PISA 2018 che misura l'alfabetizzazione finanziaria dei giovani di 15 anni in 20 Paesi (tra cui l'Italia), **il 39% degli studenti ha fatto un pagamento tramite a cellulare nei precedenti 12 mesi.**

(fonte: OCSE-Programme for International Student Assessment).

E voi?

MESCOLIAMO LE IDEE

https e lucchetto: cosa significano?

Per navigare e acquistare online in modo sicuro
sono necessarie alcune attenzioni.

Un lucchetto nella o accanto alla barra degli indirizzi del browser è l'indicatore principale
di una navigazione sicura:

non si tratta di una garanzia al 100%,
ma è un buon punto di partenza!

ANDIAMO AL PUNTO

L'icona lucchetto nella barra del browser vuol dire che:

il server ha inviato il suo **Certificato SSL (Secure Sockets Layer)** al browser;

il browser e il server si sono scambiati informazioni per **dimostrare crittograficamente che il sito sia quello indicato nel Certificato SSL;**

il browser ha verificato che il certificato del sito sia stato indirettamente firmato da una **Certification Authority (CA);**

il browser ha verificato che **il certificato SSL del sito sia valido e non scaduto;**

il browser e il server hanno condiviso **una crittografia e una chiave** per proteggere le loro comunicazioni.

Insieme al lucchetto, verrà visualizzata anche la scritta ***https://*** nella barra degli indirizzi del browser, all'inizio dell'indirizzo del sito.

Vi trovate in un ambiente decisamente sicuro!

E-commerce e piattaforme di pagamento

Quando fate shopping in un e-commerce,
utilizzare una piattaforma di pagamento intermedia
come quelle che abbiamo già citato è più sicuro rispetto
all'inserimento diretto dei dati di pagamento:
per esempio **numero di carta e codice CVC.**

ANDIAMO AL PUNTO

ANDIAMO AL PUNTO

La sicurezza non arriva solamente da fattori tecnologici: abituatevi a controllare anche la **reputazione digitale di chi state pagando.**

Alcune piattaforme (come, per esempio, Trustpilot) ci aiutano a farci un'idea sull'affidabilità di un venditore che, anche avendo tutte le carte in regola, potrebbe gestire un po' troppo "superficialmente" il proprio business, esponendoci a:

ritardi di consegna,

difficoltà nel rimborso in caso di reso,

addebiti indesiderati (più frequenti nell'acquisto di servizi).

Doppia verifica: due fattori per non avere sorprese

Le app finanziarie normalmente utilizzano verifiche **multifattoriali**:

la più diffusa si chiama **“autenticazione a due fattori” (2FA):** questa prevede che venga **aggiunto un fattore di sicurezza di qualità differente rispetto al primo**, per esempio una password e poi l’impronta digitale sul dispositivo.

Quando la doppia verifica prevede **2 inserimenti analoghi** (password + codice monouso), è più corretto parlare di **verifica in 2 passaggi (2SV)**.

3D Secure: come funziona?

Il 3D Secure delle carte di credito
(ora anche in molte carte di debito)
è un esempio di **autenticazione in due passaggi**
valida solamente per transazioni online.

Ogni volta che acquistiamo immettendo i dati di pagamento della carta, viene generato un **codice che va da 4 a 10 cifre**, da digitare in **una schermata pop-up** per finalizzare l'autorizzazione dell'addebito. **Il 3D Secure non è un PIN**: il primo è monouso, il secondo non è variabile.

Riconoscimento

Abbiamo parlato di **2 fattori o 2 step**, ma il processo di riconoscimento dell'utente in **una app finanziaria**, può prevedere anche **autenticazioni multifattoriali (MFA)**: di quali fattori parliamo?

Una cosa che sapete, ad esempio una password.

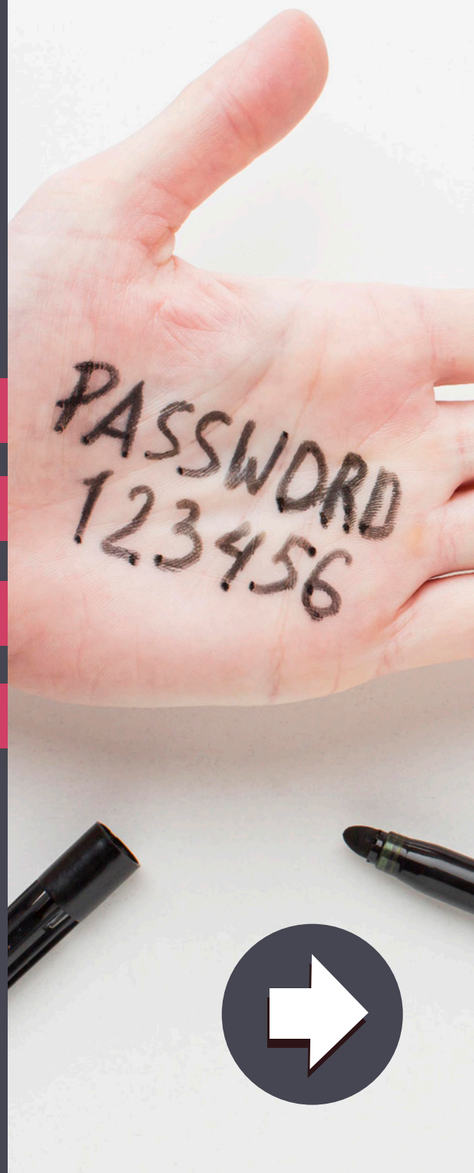
Una cosa che avete, ad esempio una smartcard o un altro dispositivo per l'autenticazione.

Una cosa che siete, ad esempio l'impronta digitale, il volto o un altro dato biometrico.

C’è password e password: come mettersi al sicuro

Condividiamo una classifica delle **bad-practice più diffuse in materia di password.**

1. **Usare sempre la solita password.**
2. Prendere nota delle password **su carta.**
3. **Scegliere la velocità** e non utilizzare l’autenticazione multifattoriale.
4. **Consentire ai browser di salvare le vostre password più importanti.**



Poi ci sono le good-practice, alcune delle quali sono:

1. **Diversificare le password;**
2. Utilizzare **password mnemoniche** (che potete anche non annotare);
3. Usare sempre **combinazioni alfanumeriche** e/o contenenti caratteri speciali.

I wallet digitali: cosa sono e come funzionano

Un wallet è un software che **memorizza in modo sicuro le informazioni di pagamento e le password, per numerosi metodi di pagamento e siti web.**

Il wallet facilita gli acquisti con la tecnologia NFC, e **consente di creare password più forti**, perché non dovremo preoccuparci di ricordarle.

In alcuni casi i wallet possono essere utilizzati anche per **archiviare carte fedeltà e coupon.**

Consensi, sicurezza e dispositivi

La vostra privacy è una **“merce” di grande valore sul web**:
si dice addirittura che **quando un servizio online**
non ha un costo, il costo siano proprio i nostri dati personali.

Quando aprite un conto, sottoscrivete una carta prepagata,
fate un acquisto, scaricate una app o aderite ad una newsletter,
vi vengono chieste molte informazioni:
alcune possono essere indirizzate a confondervi.

ANDIAMO AL PUNTO

Seguite 3 regole d'oro:

Mettete lo **slow-motion** e iniziate a leggere anche le scritte più piccole.

Autorizzate l'utilizzo dei vostri dati solamente per le finalità dirette della realtà che vi sta sottoponendo il form e **mai anche a terzi o partner**, o **per finalità differenti**.

Fate attenzione ai **flag preimpostati**!

Controllate i vostri dispositivi

Anche la corretta gestione dei propri dispositivi è fondamentale per pagamenti digitali in ambienti che, seppur virtuali, siano anche sicuri, e anche per scongiurare l'accesso di malintenzionati ai nostri dati sensibili, non soltanto finanziari.

L'utilizzo della **biometria per l'accesso al device** e ad alcune app è particolarmente efficace, ma è altrettanto importante seguire alcune "dritte":

non tenete un registro evidente di username e password nelle note del vostro telefono;

proteggete anche lo smartphone con un **anti-virus/malware/trojan**;

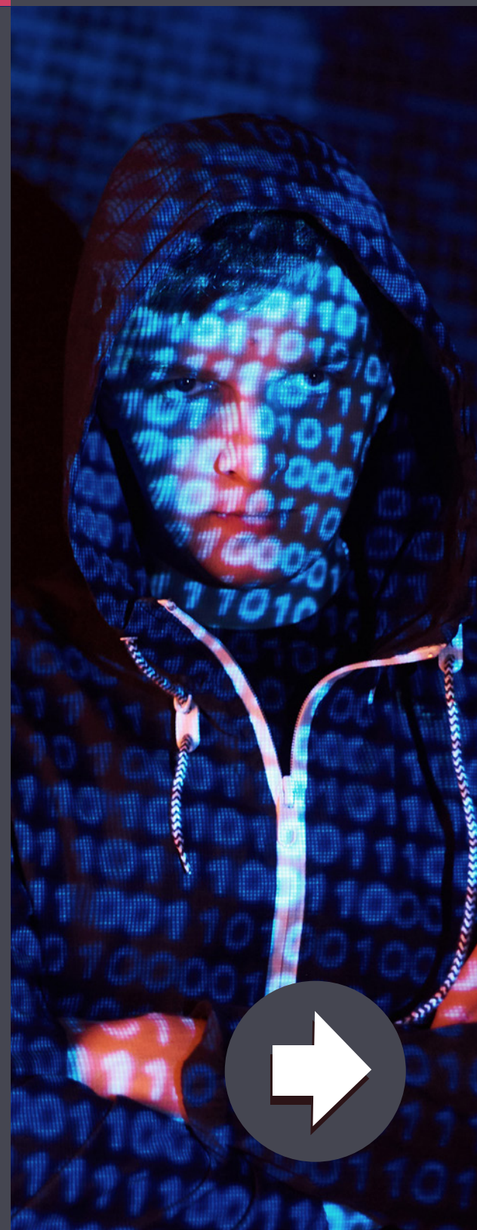
fate attenzione ai **QR-code**, e controllate che non sembrino posticci, incollati sopra un **codice preesistente**.

Phishing: truffe all'identità

Nel phishing la vittima è mandata su una **pagina di accesso falsa** dove inserisce le proprie credenziali; il cyber-criminale le inoltra alla pagina di login reale, **innescando la procedura di autenticazione: il malintenzionato cattura anche questo codice nella pagina falsa** che la vittima sta ancora utilizzando, disponendo così di **un set di autenticazione completo.**

Ora può modificare il numero di telefono a cui viene inviato il codice successivo: *e sono guai!*

ANDIAMO AL PUNTO



Che ne dite di andare nei dettagli?

Come abbiamo già accennato, il phishing è una **frode informatica** ideata allo scopo di **rubare i dati personali**, come il numero di carta di credito o le chiavi di accesso al servizio di home banking. Il phishing viene attuato da truffatori che **inviano false e-mail** apparentemente provenienti da una banca o da una società emittente di carte di credito.

Le e-mail utilizzano il logo, il nome e il layout tipico dell'azienda imitata, invitando il destinatario a collegarsi tramite un link ad un sito Internet del tutto simile a quello della banca e ad inserirvi, generalmente attraverso **una finestra pop-up che si apre dallo stesso link**, le informazioni riservate. Grazie ai dati ottenuti con l'inganno, il truffatore può effettuare transazioni bancarie a nome della vittima o sfruttare la sua carta di credito.

Un esempio di e-mail di phishing:

"Gentile utente, durante i regolari controlli sugli account non siamo stati in grado di verificare le Sue informazioni. In accordo con le regole di ... abbiamo bisogno di confermare le Sue reali informazioni. È sufficiente che Lei completi il modulo che Le forniremo. Se ciò non dovesse avvenire saremo costretti a sospendere il suo account".

Come riconoscere queste truffe?

non sono "personalizzate": la richiesta di informazioni personali è genericaed anche i motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);

sono "intimidatorie": fanno leva su una conseguenza spiacevole, ad esempio la sospensione dell'account;

non sono "situate": non riportano una data di scadenza per l'invio delle informazioni.

Mai cliccare sui link presenti in e-mail sospette:

questi collegamenti potrebbero condurvi a un sito contraffatto, indistinguibile dall'originale; anche se l'indirizzo nella barra di ricerca del browser sembra legittimo, non vi fidate: un hacker può far sì che venga mostrato un indirizzo differente rispetto a quello della pagina che state realmente visitando.

Mai cliccare sui link presenti in e-mail sospette:

Voice e phishing: vi dicono nulla? Questa nuova truffa punta ad unire la conoscenza dei dati personali degli utenti con l'utilizzo di telefonate volte ad ingannarli.

Sul cellulare o sulla casella di posta elettronica arriva una notifica, sembra arrivare dalla propria banca, e segnala operazioni sospette relative al proprio conto, così, presi dalla preoccupazione potremmo cedere alla tentazione di cliccare per saperne di più ...

A questo punto verremmo portati su un sito clone e una volta lì riceveremmo una telefonata (apparentemente credibile, anche grazie all'uso di un finto numero verde della banca) in cui i truffatori si spacciano per impiegati dell'istituto di credito che vogliono bloccare il furto. Ottenuti i codici di accesso invece, potranno autorizzare bonifici o pagamenti alle nostre spalle.

Diffidate sempre di qualunque e-mail che vi richieda l'inserimento di dati riservati: codici di carte di pagamento, chiavi di accesso al servizio home banking o informazioni personali. La vostra banca non richiederà MAI E POI MAI tali informazioni via e-mail o per telefono.