Raiffeisen
Più vicini. Più banca.

Cybersicurezza

Proteggi i tuoi dati.
Proteggi il tuo denaro.

Perché la sicurezza informatica è importante?

La cybersicurezza consiste nel proteggersi da attacchi informatici durante la navigazione in rete e il corretto utilizzo dei dispositivi per i pagamenti digitali.

In un mondo sempre più connesso, in cui operazioni bancarie, comunicazioni e acquisti avvengono online, tutelarsi è fondamentale. I criminali informatici sfruttano deliberatamente le vulnerabilità dei sistemi per accedere a informazioni riservate come **password, dati di carte di credito** o **coordinate bancarie,** e i tentativi di frode ai danni della clientela sono in costante aumento. Particolarmente insidiose sono **e-mail, SMS, telefonate** o **siti web contraffatti** che sembrano provenire da mittenti affidabili.

CLICCARE FRETTOLOSAMENTE, CONDIVIDERE LE **PROPRIE CREDENZIALI** O COMUNICARE UN **PIN** PUÒ CAUSARE CONSEGUENZE IMPORTANTI.

Per questo è importante sapere riconoscere le situazioni di rischio. La tua banca è sempre pronta a supportarti nella lotta alle frodi!

Le truffe più comuni

- **Phishing** via e-mail
- **Truffe sui social media**
- **Smishing** via SMS
- **Negozi online fasulli**
- **Vishing** via telefono
- **Accesso non autorizzato tramite software di assistenza remota**
- **Frodi finanziarie e di investimento**
- **Concorsi a premi fraudolenti**

Importante

Non divulgare mai informazioni riservate come PIN, password, numeri di carta di credito e simili tramite e-mail, SMS o telefonate.

Nessuna banca contatta i propri clienti per richiedere credenziali di accesso o altri dati sensibili.

Le principali minacce informatiche

Come riconoscerle,
cosa si rischia e come difendersi

Phishing

Di cosa si tratta?

IL PHISHING È UNA DELLE TECNICHE DI FRODE PIÙ DIFFUSE IN RETE.

I truffatori inviano **e-mail** che sembrano comunicazioni ufficiali di banche o aziende note, contenenti un **link** che rimanda a un **sito contraffatto,** molto simile a quello autentico.

Quali sono le conseguenze?

Se si inseriscono le proprie **credenziali** su tale sito, queste finiscono direttamente nelle **mani dei truffatori,** che possono così accedere all'online banking e predisporre bonifici.
I trasferimenti vengono eseguiti solo dopo che la vittima li ha autorizzati dal proprio dispositivo.

Come riconoscerlo?

Segnali tipici sono **errori ortografici o di formattazione,** indirizzi e-mail insoliti o URL scritti in modo leggermente scorretto. Spesso i malintenzionati esercitano pressione psicologica, ad esempio minacciando il blocco del conto.

Come difendersi?

- **Non aprire link** contenuti in **e-mail sospette.**
- Non inserire **credenziali** come nome utente, password, PIN o OTP.
- Verifica con attenzione **mittente** e **indirizzo web.**
- In caso di dubbio, contatta immediatamente la tua Cassa Raiffeisen.

Smishing

Di cosa si tratta?

UNA FORMA DI PHISHING CHE UTILIZZA IL CANALE DEL **SMS.**

I messaggi sembrano provenire direttamente dalla banca o dall'emittente della carta di credito e contengono un **link** a un sito fasullo oppure un **numero di telefono** con l'invito a richiamare.

Quali sono le conseguenze?

Una volta inserite le credenziali, i truffatori possono **accedere all'online banking** e predisporre bonifici, eseguiti solo dopo l'autorizzazione da parte della vittima.

Come riconoscerlo?

Il messaggio genera **ansia** o senso di **urgenza**, ad esempio segnalando un pagamento sospetto o un accesso da un dispositivo sconosciuto.
Il link può sembrare autentico, ma spesso è scritto in modo scorretto, così come il testo del messaggio: **refusi o errori grammaticali** sono un chiaro segnale d'allarme.

I **mittenti** si spacciano spesso per istituti noti come Nexi, Raiffeisen o Booking, oppure utilizzano numeri esteri (es. Lugano, Lisbona) o sconosciuti.

Come difendersi?

- **Non aprire link** contenuti negli SMS.
- Non richiamare il **numero** indicato nel messaggio.
- Non inserire **dati** personali o riservati.
- Valuta **con occhio critico** messaggi dal tono allarmante.
- In caso di sospetto, contatta immediatamente la tua Cassa Raiffeisen.

Vishing

Di cosa si tratta?

I TRUFFATORI CONTATTANO LE VITTIME **TELEFONICAMENTE.**

Spacciandosi per impiegati di banca o di altri enti affidabili, riferiscono di presunti problemi con il conto corrente.

Quali sono le conseguenze?

Comunicando credenziali di accesso o password di autorizzazione, si rischia di essere inconsapevoli complici dei frodatori.

Come riconoscerlo?

Nessuna banca legittima richiede mai le **credenziali dell'online banking** per telefono. I truffatori fanno inoltre leva sull'**urgenza**, chiedendo di autorizzare operazioni "necessarie" per **bloccare pagamenti** in corso.

Come difendersi?

- Non comunicare mai **password** o **PIN** al telefono.
- In caso di dubbio, **interrompi** subito **la chiamata.**
- Segnala l'accaduto alla tua Cassa Raiffeisen.

Frodi finanziarie e di investimento

Di cosa si tratta?

I CRIMINALI SI PRESENTANO CON ALLETTANTI **OPPORTUNITÀ DI INVESTIMENTO**, PROMETTENDO **RENDIMENTI ELEVATI A FRONTE DI RISCHI MINIMI.**

Le offerte vengono diffuse tramite siti web, e-mail, telefonate o inserzioni sui social media e riguardano **azioni, criptovalute, immobili o altri prodotti finanziari.**

Quali sono le conseguenze?

Le vittime rischiano **perdite economiche considerevoli**: il denaro trasferito ai truffatori è in genere irrecuperabile e i guadagni promessi non si materializzano.

Come riconoscerle?

Le offerte garantiscono **rendimenti elevati** in tempi brevi e **senza alcun rischio**, facendo pressione affinché si investa subito per non perdere un'opportunità irripetibile.

La richiesta di **dati personali o finanziari** e l'assenza di **informazioni aziendali chiare** o di **documentazione ufficiale** rappresentano ulteriori segnali d'allarme.

Come difendersi?

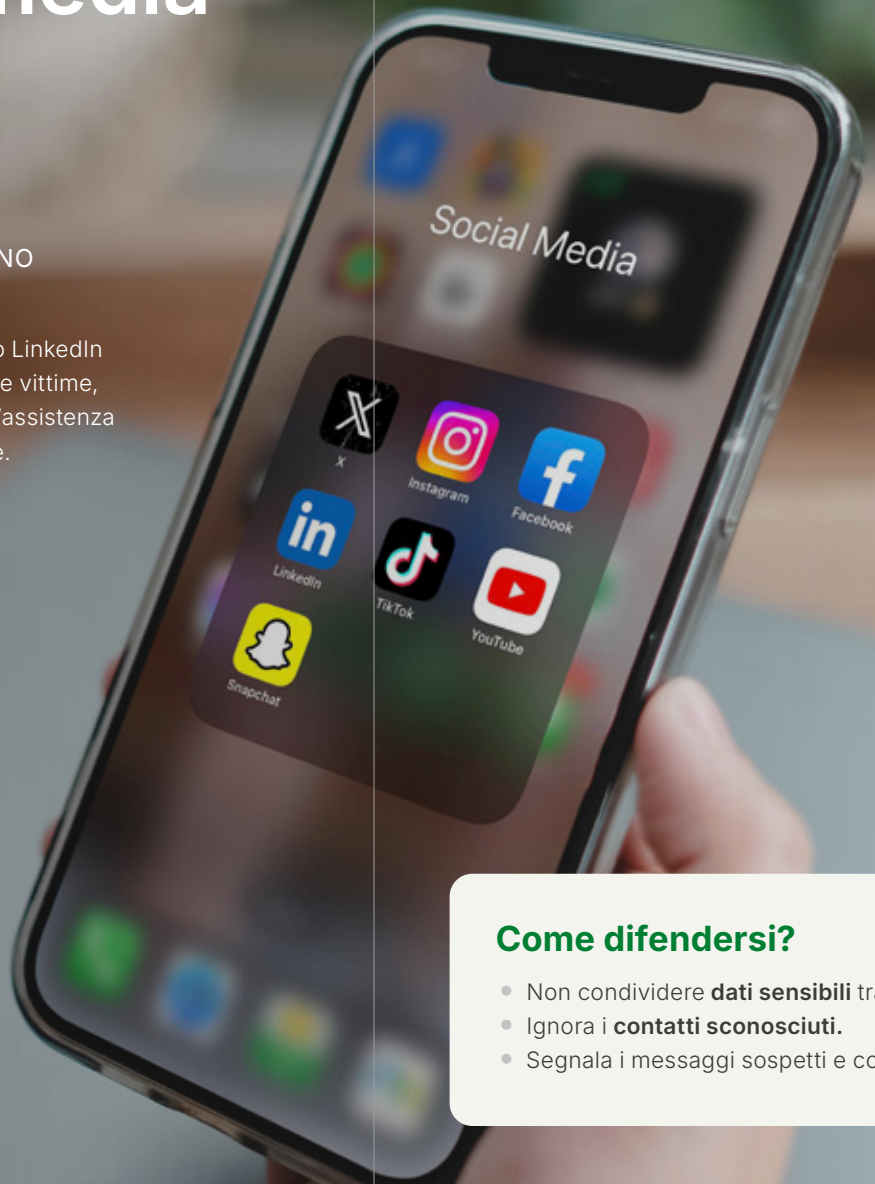
- **Diffida delle offerte** troppo allettanti per essere vere.
- Verifica sempre **l'affidabilità** dell'azienda o della persona che propone l'investimento, consultando fonti attendibili o recensioni.
- Non fornire mai dati personali o finanziari prima di aver verificato **l'autenticità dell'offerta.**

Truffe sui social media

Di cosa si tratta?

I TRUFFATORI UTILIZZANO **SOCIAL NETWORK**

quali Facebook, Instagram o LinkedIn per entrare in contatto con le vittime, spacciandosi per addetti all'assistenza clienti o persone conosciute.



Quali sono le conseguenze?

Tramite link o messaggi fraudolenti vengono sottratte le **credenziali di accesso,** consentendo ai malintenzionati di utilizzare il **profilo in modo illecito.**

Come riconoscerle?

Profili sconosciuti richiedono **dati personali o finanziari** oppure invitano a cliccare su link sospetti.

Come difendersi?

- Non condividere **dati sensibili** tramite social network.
- Ignora i **contatti sconosciuti.**
- Segnala i messaggi sospetti e contatta la tua banca.

Negozi online fasulli

Di cosa si tratta?

I CRIMINALI GESTISCONO **E-COMMERCE FRAUDOLENTI** CON **OFFERTE APPARENTEMENTE VANTAGGIOSE**

e richiedono dati di pagamento o della carta di credito al momento dell'acquisto.

Quali sono le conseguenze?

La merce ordinata **non viene consegnata** oppure i dati di pagamento vengono utilizzati per **addebiti non autorizzati.**

Come riconoscerli?

Assenza di note legali, nessun indirizzo aziendale, **pagamento anticipato** come unica opzione disponibile o **sconti esagerati.**

Come difendersi?

- Verifica il **venditore** e le **note legali.**
- Fai acquisti solo su **siti web conosciuti e affidabili.**
- Controlla la presenza di **"https"** nell'indirizzo web: la "s" sta per "sicuro".
- Leggi le **recensioni.**
- In caso di frode, blocca immediatamente la carta e informa la tua banca.

Come tutelarsi dagli attacchi informatici

La sicurezza dei dati personali acquista sempre maggiore rilevanza.

Le seguenti regole ti aiuteranno a difenderti dalle diverse forme di truffa.

- Apri e-mail o SMS solo se sei certo o certa dell'**autenticità del mittente,** verificando con attenzione l'indirizzo.
- Non richiamare mai **numeri di telefono** indicati in SMS provenienti da mittenti sconosciuti.
- Non scaricare **allegati** da e-mail sospette prima di aver verificato la provenienza.
- **Non cliccare su link** contenuti in messaggi sospetti. Se lo hai già fatto, non effettuare il login sul sito contraffatto e chiudi immediatamente il browser.
- Utilizza sempre **password complesse e diverse** per ogni servizio.
- **Attenzione:** la banca non ti chiederà mai le credenziali per l'accesso al tuo Raiffeisen Online Banking.
- Tieni **segreti i dati di accesso** al tuo online banking.
- Verifica con attenzione gli **estremi di ogni operazione** prima di confermarla. Se arrivano notifiche push sospette, rifiutale.
- Presta particolare attenzione alle operazioni che riportano termini come **"in tempo reale"** o **"bonifico istantaneo"** e verifica attentamente la causale.

Cosa fare in caso di truffa?

- Mantieni la **calma** e **contatta** immediatamente la tua **banca.**
- **Blocca senza indugio la carta di debito o di credito** e l'accesso all'**online banking.**
- Segnala tempestivamente eventuali **bonifici sospetti.**
- Cambia tutte le **credenziali di accesso e le password** dei tuoi account.
- Conserva **screenshot e altre prove** – e-mail, SMS o numeri di telefono – per consentire successive verifiche o segnalazioni.
- Non inoltrare **e-mail sospette.**
- Segnala **e-mail di phishing** alla tua Cassa Raiffeisen o all'indirizzo phishing@raiffeisen.it, quindi elimina immediatamente il messaggio sospetto.
- In caso di **furto di identità e di bonifici non riconosciuti,** sporgi denuncia presso le autorità di polizia.

- **Controlla regolarmente l'estratto conto** e segnala immediatamente eventuali movimenti sospetti.
- **Non utilizzare reti Wi-Fi pubbliche per operazioni bancarie,** in quanto sono più vulnerabili agli attacchi informatici.
- In caso di **furto o smarrimento** di smartphone, tablet o carte legate al conto, blocca immediatamente **l'accesso** all'online banking e **l'utilizzo** delle carte, e contatta la tua Cassa Raiffeisen.
- **Ricorda:** le autorità pubbliche non chiedono mai di trasferire il proprio denaro su cosiddetti **"conti sicuri"** in presenza di presunte irregolarità. Questi conti **non esistono**: sono un'invenzione dei truffatori per indurvi a effettuare un bonifico.

La testimonianza di un cliente Raiffeisen

“Saluti da San Lugano”

Un cliente di una Cassa Raiffeisen altoatesina, tecnico di professione e con solide conoscenze informatiche, ha ricevuto un SMS, apparentemente inviato dal gestore di pagamenti **Nexi.**
Il messaggio lo informava di un addebito sulla sua carta di credito avvenuto a San Lugano e lo invitava a chiamare il numero indicato qualora non avesse autorizzato l’operazione.

Il cliente ha chiamato e un sedicente operatore Nexi si è offerto di aiutarlo a bloccare il presunto addebito non autorizzato, dichiarando di aver bisogno prima del **nome utente e poi della password.** Messo sotto pressione con la minaccia che il pagamento sarebbe andato a buon fine senza un intervento immediato, il cliente ha dapprima rivelato parte del suo nome utente.

Quando però gli è stato chiesto di fornire anche le credenziali complete dell’online banking, ha riagganciato, ignorato le chiamate successive e **bloccato immediatamente la carta.**

Il tentativo di frode è stato poi confermato dalla Cassa Raiffeisen, che ha adottato prontamente le misure di sicurezza necessarie.

Truffe e avvisi di sicurezza aggiornati

Climaticamente neutrale
Stampa
ClimatePartner.com/14583-1805-1002

Edizione: maggio 2026