

Scheda per insegnanti n. 3 · Scuola secondaria di primo grado

Come si riconosce una truffa online?

Una lezione su messaggi falsi, siti trappola e codici da non dare mai

Classi	Durata	Materiali	Costo
I, II e III media	50 minuti	LIM o proiettore, scheda studente	Gratuito, nessuna registrazione

In breve. Le truffe online più diffuse non "bucano" i computer: convincono le persone a dare un codice o a fare un pagamento. Secondo il rapporto congiunto dell'Autorità bancaria europea e della BCE del dicembre 2025, nel 2024 le frodi sui pagamenti nello Spazio economico europeo sono state di 4,2 miliardi di euro, e sui bonifici circa l'85% delle perdite è ricaduto sugli utenti, soprattutto a causa di raggiri che li hanno spinti a fare loro stessi il pagamento. Riconoscere i segnali è la prima difesa.

Obiettivi di apprendimento

Al termine della lezione lo studente:

- riconosce i tre segnali tipici di un messaggio truffa: fretta, link da cliccare, richiesta di codici;
- distingue phishing (email), smishing (SMS e chat) e vishing (telefonate);
- riconosce le trappole tipiche dei giochi e degli acquisti online: regali troppo belli, venditori che chiedono pagamenti fuori dalla piattaforma;
- sa cosa fare se ha già cliccato o dato un codice: avvisare subito un adulto, bloccare la carta, segnalare.

Collegamento con le Linee guida per l'educazione civica

Educazione civica. La legge 5 marzo 2024 n. 21 ha inserito l'educazione finanziaria tra i temi dell'insegnamento di educazione civica (legge 92/2019). Le Linee guida del 2024 la collocano nel nucleo "Sviluppo economico e sostenibilità", con attenzione alla tutela del risparmio e alle tecnologie digitali di gestione del denaro.

Collegamenti trasversali. Italiano (analisi di un testo persuasivo), Tecnologia (link, siti, indirizzi web), Matematica (lettura di dati e percentuali).

Cosa serve

- Il fumetto **Il messaggio che sembra della banca**: www.raccontocorrente.it/storie/il-messaggio-che-sembra-della-banca
- Il fumetto **Perché il PIN ha 5 cifre?**: www.raccontocorrente.it/storie/perche-il-pin-ha-5-cifre
- La scheda studente (pagina 3 di questo file), una copia per alunno

Nota per il docente. I messaggi della scheda sono esempi inventati a scopo didattico e non si riferiscono a banche o aziende reali. Raccontocorrente non consiglia prodotti e non raccoglie dati degli studenti.

Svolgimento della lezione

Tempo	Attività	Suggerimenti
5'	**La domanda di partenza.** "Vi è mai arrivato un messaggio strano, un regalo troppo bello o un link da un numero sconosciuto?" Raccogliere esperienze senza chiedere dettagli personali.	Tenere un clima senza giudizio: chi è caduto in una truffa non deve vergognarsi.
10'	**Il fumetto.** Lettura a voci alterne di "Il messaggio che sembra della banca" e individuazione dei tre segnali.	Scrivere alla lavagna: FRETTA, LINK, CODICI.
10'	**Le facce della truffa.** Presentare la tabella qui sotto con i canali e le trappole più comuni.	Collegare ai giochi online: account, oggetti, valute virtuali.
20'	**Scheda studente.** Esercizi 1-4 a coppie: ogni coppia fa da "detective".	L'esercizio 5 può diventare compito a casa.
5'	**Il piano di emergenza.** La classe scrive i passi da fare se si è già cliccato.	Atteso: avvisare un adulto, bloccare la carta, cambiare password, segnalare.

Le facce della truffa

Nome	Canale	Come si presenta
Phishing	Email	Sembra la banca, un negozio o un servizio famoso. Chiede di cliccare per "verificare" o "sbloccare".
Smishing	SMS e chat	Un avviso urgente con un link: pacco in giacenza, conto bloccato, premio da ritirare.
Vishing	Telefonata	Qualcuno finge di essere la banca o le forze dell'ordine e chiede codici o un bonifico "di sicurezza".
Falsi regali nei giochi	Giochi e social	Valuta virtuale o oggetti gratis in cambio delle credenziali dell'account.
Falsi venditori	Annunci online	Prezzo molto basso e richiesta di pagare fuori dalla piattaforma, con ricarica o bonifico.

Le tre regole che valgono sempre. Nessuna banca chiede PIN, password o codici per messaggio, email o telefono. Non si clicca su link arrivati all'improvviso: si apre l'app o il sito ufficiale scrivendo l'indirizzo. Se qualcosa mette fretta, ci si ferma e si chiede a un adulto.

Domande per la discussione

1. Perché chi truffa mette fretta?
2. Perché le truffe imitano proprio banche, corrieri e giochi famosi?
3. Cosa rende difficile chiedere aiuto dopo essere caduti in una truffa? Come possiamo renderlo più facile?



Detective delle truffe: la mia scheda

Nome _____ Classe _____ Data _____

1. Trova i segnali di allarme. Sottolinea fretta, link e richiesta di codici

"BANCA XY: il tuo conto è stato sospeso. Clicca entro 15 minuti su www.bancaxy-verifica.co e inserisci il codice che ricevi."

"Complimenti! Hai vinto 5.000 gemme nel tuo gioco preferito. Per riceverle scrivi qui nome utente e password."

Messaggi inventati a scopo didattico.

2. Vero o falso?

Frase	V / F
Se il messaggio compare nella stessa chat dei messaggi veri della banca, allora è sicuramente vero.	
La banca non chiede mai il PIN per telefono.	
Un venditore che chiede di pagare fuori dalla piattaforma è un segnale di allarme.	
Se ho già cliccato, è meglio non dirlo a nessuno.	

3. Collega ogni nome al suo canale

A. Phishing
B. Smishing
C. Vishing

__ Telefonata
__ Email
__ SMS o chat

4. Cosa fai? Scrivi la tua mossa

Ricevi una telefonata: "Sono della sua banca, abbiamo visto un pagamento sospetto. Per bloccarlo mi detti il codice che le arriva adesso per SMS."

_____

_____

5. Il piano di emergenza: se ho già cliccato o dato un codice, cosa faccio? Scrivi tre passi

_____

_____

_____

Soluzioni e valutazione

1. Primo messaggio: fretta ("entro 15 minuti"), link a un indirizzo che imita quello della banca, richiesta del codice. Secondo messaggio: premio troppo bello, richiesta di nome utente e password.

2. Vero o falso: F (i messaggi falsi possono comparire nella stessa conversazione di quelli veri), V, V, F.

3. Collegamenti: C telefonata, A email, B SMS o chat.

4. Non dettare nessun codice, chiudere la telefonata, avvisare un adulto e, se serve, richiamare la banca al numero ufficiale scritto sulla carta o nell'app.

5. Risposta aperta. Elementi attesi: avvisare subito un genitore; bloccare la carta chiamando la banca; cambiare la password dell'account; segnalare alla Polizia Postale, anche online sul portale del Commissariato di P.S. online (www.commissariatodips.it).

Griglia di osservazione

Criterio	Iniziale	Base	Intermedio	Avanzato
Riconoscimento	Non nota i segnali	Nota un segnale	Nota i tre segnali	Spiega perché sono segnali di truffa
Lessico	Non conosce i termini	Usa "truffa" e "link"	Distingue phishing, smishing e vishing	Usa i termini e li spiega con parole sue
Comportamento	Risponde o clicca	Non clicca	Non clicca e avvisa un adulto	Sa anche come segnalare e bloccare
Collaborazione	Lavora da solo	Partecipa se sollecitato	Contribuisce nella coppia	Guida la coppia e argomenta

Fonti e note

Autorità bancaria europea e Banca Centrale Europea, rapporto congiunto sulle frodi nei pagamenti, comunicato del 15 dicembre 2025 (dati 2024). Polizia Postale e delle Comunicazioni, portale del Commissariato di P.S. online: www.commissariatodips.it. Legge 5 marzo 2024 n. 21, art. 25, che modifica la legge 20 agosto 2019 n. 92. Linee guida per l'insegnamento dell'educazione civica, DM 7 settembre 2024 n. 183.



Hai usato questa scheda in classe? Segnalaci errori o idee per nuove lezioni: ogni suggerimento degli insegnanti ci aiuta a migliorare. Nuove schede gratuite su **www.raccontocorrente.it/insegnanti/**