INTERNET
I PERICOLI DA EVITARE

Consigli pratici per non cadere nelle truffe e altri inganni

Federconsumatori
Friuli Venezia Giulia

INTERNET
I PERICOLI DA EVITARE

Consigli pratici per non cadere nelle truffe e altri inganni

a cura di
Emanuela Pitassi

Coordinamento
Marco Missio

L'immagine in copertina è di Federico Missio
Le altre immagini sono tratte da internet

Federconsumatori
Friuli Venezia Giulia

INDICE

■ **Presentazione** 5

■ **Introduzione** 7

■ **PHISHING** 8
- La truffa del principe nigeriano 8
- PHISHING tramite SMS - smishing 9
- PHISHING su WhatsApp 9
- PHISHING su Instagram 10

■ **FRODI SULL'ACQUISTO DI PRODOTTI O SERVIZI** 11
- La frode delle polizze assicurative 11
- Frodi sull'acquisto di biglietti per eventi sportivi o concerti 12
- La frode del vaglia postale - Postamat 13
- Romantic scam - la truffa sentimentale 15
- Decalogo antitruffa: consigli generali per tutelarsi da phishing e scammer online e su dispositivi mobili 16

■ **FORME DI PAGAMENTO SICURO** 18
- Le forme di pagamento classiche 18
- Canali o gateway di pagamento 19
- I 10 gateway di pagamento più utilizzati per permettere acquisti online sicuri 19
- 5 passi da seguire per assicurarsi di effettuare pagamenti su siti di e-commerce sicuri 22

■ **ADESCAMENTO ONLINE DI MINORENNI** 23
- Modalità di adescamento 24
- Vademecum ragazzi 26
- Vademecum genitori 27

■ **Contatti utili** 29

PRESENTAZIONE

Può sembrare superata l'idea di stampare un vademecum per aiutare il consumatore a difendersi dai pericoli che si trovano in agguato quando ci si connette a internet, poiché fissare su carta una materia che è in continua evoluzione rischia di rendere la pubblicazione vecchia in un batter d'occhio. Bisogna inoltre considerare che in rete si trova molto materiale sull'argomento, pubblicato in vari siti, e dunque apparentemente si rafforza l'interrogativo: a cosa serve una guida?
In realtà, anche se le modalità in cui avvengono le truffe si rinnovano di continuo, le cautele da adottare per evitare di essere raggirati si fondano su principi che restano sempre validi, e infatti non differiscono sostanzialmente col passare del tempo. Facciamo un esempio: se la finalità del truffatore è carpire le vostre credenziali di accesso al conto corrente online, con il tempo le mail e i siti-clone si sono sempre più raffinati e sono diventati sempre più ingannevoli, ma il consiglio di accedere al proprio conto online dal proprio browser e mai da link presenti in una mail ricevuta resta sempre valido.
Alla seconda obiezione rispondiamo che i consigli che si trovano in rete sono molto spesso ristretti all'argomento trattato dal sito (sui siti delle banche troviamo consigli per salvaguardare le nostre credenziali del conto, sul sito della Consob per effettuare investimenti finanziari sicuri, sul sito dove prenoti alloggi per evitare di pagare prenotazioni fasulle, etc.). Qui, senza la pretesa di essere esaustivi, abbiamo cercato di occuparci delle truffe che vanno dalle mail, ai siti, alle chat, ai Social Network fino all'odioso reato dell'adescamento di minori.
Anche con questa piccola pubblicazione Federconsumatori FVG cerca di aiutare le famiglie, i giovani e i meno giovani a districarsi in un mondo in cui è sempre più difficile riuscire a farlo contando solo sulle proprie forze.

Angelo D'Adamo
Presidente Federconsumatori FVG

INTRODUZIONE

Sempre più raffinate ed evolute, spesso difficili da individuare, le truffe online continuano a mietere un numero impressionante di vittime.
I cybercriminali, approfittando dei sentimenti, dei bisogni e delle emozioni umane quali paura, avidità ed empatia, ma anche dell'ingenuità della maggior parte degli utenti di Internet, hanno solitamente due obiettivi principali:

1. l'estorsione di denaro;
2. il furto di dati personali da poter utilizzare in un secondo momento per commettere ulteriori reati.

Ecco perché conoscere le principali tecniche adottate da questi "malviventi digitali" permette di comprendere innanzitutto i rischi in cui si può incorrere inconsapevolmente e, di conseguenza, quali strategie adottare per evitare di cadere nella loro trappola.
Questa guida informativa illustra le più comuni, e purtroppo più diffuse, truffe online e fornisce dei consigli pratici, dei veri e propri vademecum, per i navigatori del Web.
È possibile individuare due macro-categorie di truffe online, di seguito analizzate nel dettaglio:

1. Phishing
2. Frodi (in inglese meglio note come *scam*)

Successivamente, verranno analizzate le modalità di pagamento sicuro online: saperle riconoscere è il primo passo per evitare di cadere nella rete di cybercriminali.
L'ultima sezione della guida è invece interamente dedicata all'aberrante crimine di adescamento online di minori: verranno illustrate le più comuni tecniche di adescamento di giovani e giovanissimi navigatori, verranno riportati consigli pratici a loro dedicati, ma anche ai genitori spesso non pienamente consapevoli delle attività svolte in Rete dai loro figli e dei reali rischi nei quali possono incorrere.

PHISHING

La truffa nota come ***phishing*** esiste da più di una decade, ma continua a mietere vittime visto che nel corso degli anni è diventata via via più raffinata, facendo leva soprattutto sul desiderio di autocelebrazione ed esclusività degli utenti del Web.
Come funziona esattamente?
Il truffatore, attraverso una e-mail dall'aspetto professionale, induce il malcapitato a cliccare su un link: il collegamento ipertestuale che induce l'utente all'azione fa riferimento a URL solitamente lunghi, difficilmente leggibili e incomprensibili, oppure a URL molto simili a quelli originali che differiscono per pochi caratteri. A questo punto si apre una pagina Web costruita ad hoc che, per ingannare facilmente l'utente, sembra affidabile e realizzata proprio da note compagnie e aziende di settore.
Lo scopo principale del truffatore è **ottenere informazioni personali** come la carta di credito, ma sempre più spesso l'obiettivo è la raccolta di documenti personali (come la fotocopia della carta di identità) che rappresentano una ghiotta possibilità per il malvivente di effettuare un vero e proprio **furto di identità** con conseguente utilizzo fraudolento dei dati, che possono essere sfruttati per compiere ulteriori reati. **Occorre quindi prestare estrema attenzione a queste sedicenti email ed evitare nel modo più assoluto di cliccare sui link presenti in esse.** Di seguito sono descritte alcune tra le truffe più note, perfino 'famose', che tuttavia continuano a colpire ancora molti utenti.

La truffa del principe nigeriano

Altresì nota come *SCAM419* consiste in una e-mail nella quale tipicamente a scrivere è un principe nigeriano, o un funzionario governativo, che offre al malcapitato l'opportunità di ingenti guadagni finanziari a fronte del pa-

gamento di una piccola parte del capitale da investire. Nella e-mail c'è un link che rimanda a una pagina Web creata appositamente per inserire i dati del proprio conto corrente bancario, oppure per effettuare il versamento di una cifra (solitamente da qualche centinaio di euro a qualche migliaio). Ovviamente, se l'importo iniziale viene versato, va completamente perso e non si riceve alcun guadagno in cambio.

PHISHING tramite SMS - smishing

Anche in questo caso il truffatore utilizza una contraffazione attraverso la quale richiede di cliccare su un link che ha come destinazione una pagina Web trappola, la differenza è il mezzo: il tradizionale **SMS**. Si sfruttano meccanismi psicologici come l'urgenza o l'ottenimento di un vantaggio personale, oltre alla sensazione di maggiore fiducia che l'SMS tende a indurre nel malcapitato. Ciononostante l'obiettivo dei truffatori è sempre lo stesso: rubare informazioni personali quali password e numeri di carte di credito per scopi illegali.

PHISHING su WhatsApp

WhatsApp, nata come applicazione di Instant Messaging, ossia di Messaggi Istantanei, è stata acquistata da Facebook nel 2014 e da allora il numero di utenti attivi continua ad aumentare esponenzialmente: ad oggi sono più di **1,5 miliardi gli utenti** attivi che scambiano circa **60 miliardi di messaggi al giorno**. Indubbiamente una ghiotta opportunità per truffatori in agguato, attenti a colpire specialmente i più giovani utilizzatori di questa applicazione. Come avvengono i tentativi di phishing in questo caso?

- ***Messaggio truffa di pagamento del servizio:*** torna ciclicamente su WhatsApp, nonostante lo staff dell'applicazione di messaggistica abbia più volte smentito ogni possibilità di pagamento. Il messaggio contiene un link che porta al pagamento di una somma per poter continuare a utilizzare WhatsApp. Una variante più recente consiste nel messaggio truffa del pagamento del servizio per ottenere ***WhatsApp Premium***: è bene ricordare che non esiste alcuna versione ***Gold*** o ***Premium*** dell'applicazione.
- ***Messaggio truffa del buono sconto***: si riceve un messaggio che ripor-

ta un link per ottenere immediatamente un importante buono sconto di qualche nota catena di supermercati o di qualche marchio blasonato. Dopo aver premuto sul link, apparentemente, non sembra accadere nulla: tuttavia la vittima in questo caso scarica inconsapevolmente sullo smartphone un virus che monitorerà le sue attività e abitudini. Occorre quindi ricordare che **le aziende non offrono mai buoni sconto su WhatsApp**. Diffidare da messaggi che non seguono canali di comunicazione tradizionali come email ed SMS (per ricevere i quali, l'utente deve comunque aver prestato il consenso in sede di sottoscrizione del servizio, come nel caso di sottoscrizione di una tessera fedeltà del negozio/supermercato).

PHISHING su Instagram

Non solo gli utenti di WhatsApp, ma anche di Instagram, il Social Network che ha raggiunto gli 895 milioni di utenti attivi in tutto il mondo, sono vittime designate di phishing. Se improvvisamente un noto influencer inizia a promettere regali in cambio di un clic, occorre fare attenzione: chi si nasconde realmente dietro queste accattivanti promesse? Si tratta di account falsi, o meglio, di account rubati! Ultima frontiera delle truffe ai danni di utenti dei Social Network, è la truffa che ruba gli account di Instagram. I cybercriminali si impossessano degli account delle vittime attraverso attacchi di phishing che impediscono la successiva riattivazione dell'account.

Come funziona? L'utente Instagram riceve una e-mail dalle sembianze ufficiali contenente il messaggio "Il tuo account è stato cancellato definitivamente per violazione del copyright". Facendo clic si viene reindirizzati su una pagina di phishing molto convincente: essa contiene un'immagine in cui si comunica di avere a cuore la protezione del copyright e si propone un link per proseguire e inserire i propri dati. Una volta inseriti però l'account viene rubato e, anche se l'utente tenta il processo di riattivazione, l'account resta in mano al truffatore. Gli account oggetto della truffa sono solitamente quelli con un numero di follower elevato, superiore ai 15.000 (tra le vittime si riporta il caso di diversi attori, cantanti, fotografi e influencer). Al furto dell'account seguono tentativi di estorsione: una volta entrati in possesso del profilo, i criminali possono utilizzare tutto il materiale dell'account, oltre a chiedere fotografie di nudo o video per restituire l'account.

FRODI SULL'ACQUISTO DI PRODOTTI O SERVIZI

Chi commette una frode informatica, reato inserito nel codice penale già nel 1993, *"altera o interviene su un sistema informatico o telematico, o anche su dati, informazioni o programmi, conseguendo un ingiusto profitto, con altrui danno"*. Le frodi possibili sono tante quante le possibilità di acquisto di servizi o prodotti attraverso siti e portali Web.

Di seguito sono descritte le frodi online più comuni, perpetrate a danno di ignari acquirenti, ma anche di venditori di prodotti e/o servizi sulla Rete.

La frode delle polizze assicurative

L'Istituto di vigilanza delle Assicurazioni ha recentemente scoperto un giro d'affari di 3 milioni di euro e un centinaio di siti Web falsi che, grazie a nomi apparentemente affidabili (es. www.assicurazionidirect.it), nascondevano in realtà delle vere e proprie truffe ai danni dei malcapitati. La frode è semplice: il malcapitato compila un modulo completo di tutti i suoi dati, effettua il pagamento della polizza (magari attraverso strumenti di trasferimento di denaro), ma in cambio non ottiene alcuna assicurazione. Si tratta di una frode piuttosto subdola, in quanto le promozioni si presentano particolarmente vantaggiose e accattivanti, dalla parvenza 'istituzionale' e possono arrivare attraverso e-mail, ma anche essere presenti sui motori di ricerca tramite appositi banner, o come post sponsorizzati sui Social Network. Le vittime hanno solitamente scarsa dimestichezza con gli strumenti finanziari e assicurativi; anche i *millennials* sono spesso vittime di queste truffe perché principalmente attratti dal notevole risparmio proposto dalla falsa polizza assicurativa.

Come tutelarsi quindi?

Ecco 5 consigli pratici per non cadere nella trappola delle frodi assicurative:

1. **Controllare** che la compagnia assicurativa sia inserita nell'elenco delle compagnie autorizzate IVASS e che all'inizio dell'indirizzo

del sito compaia l'acronimo ***https***, indice di maggiore sicurezza nella comunicazione tra siti Web;

2. Se il preventivo è offerto da un **intermediario**, **verificare** che sul suo sito siano presenti **i dati identificativi obbligatori** per legge (ad es. il numero di iscrizione al Registro Unico Intermediari) e che lo stesso intermediario sia presente sul Registro Unico degli Intermediari assicurativi e riassicurativi;
3. Diffidare dalle comunicazioni tramite WhatsApp: una compagnia assicurativa utilizza canali di comunicazione ufficiali. **Evitare nella maniera più assoluta l'invio di dati sensibili via WhatsApp**.
4. **Effettuare esclusivamente pagamenti tracciabili**: dubitare di chi propone sconti imperdibili se si effettua, anziché un bonifico, la ricarica di una carta prepagata o il trasferimento di denaro. Controllare che, a pagamento effettuato, tutti i documenti relativi all'acquisto della polizza vengano recapitati via e-mail.
5. **Verificare** che tutte **le informazioni contrattuali** siano corrette e che la **polizza sia stata attivata**. Nel caso di polizza assicurativa RCA, inserire la targa del veicolo sul Portale dell'Automobilista e controllare l'attivazione della polizza: qualora non fosse stata attivata alcuna polizza, contattare immediatamente la Polizia Postale o l'Istituto per la Vigilanza.

Frodi sull'acquisto di biglietti per eventi sportivi o concerti

Un'ulteriore frode di cui sono sempre più vittime i giovani riguarda la vendita a prezzi stracciati di biglietti per eventi sportivi o musicali, particolarmente esclusivi, e per i quali è noto che c'è già da tempo il 'tutto esaurito'. Si stima che il 10% dei *millennials* siano vittime di frodi sull'acquisto di biglietti.

Anche in questo caso, la sponsorizzazione di questi falsi biglietti può avvenire attraverso diversi canali: si riceve una e-mail contenente il link al sito contraffatto, oppure si clicca su un banner pubblicitario, e così via. La vittima, attratta dalla possibilità di risparmiare sul prezzo del biglietto o di ottenere incredibilmente un biglietto per un concerto già *sold-out*, cliccando sul link accede a una pagina Web completamente contraffatta, seppur apparentemente affidabile e molto simile ai canali di vendita ufficiali. Peccato che si tratti

di un imbroglio e che al termine della transazione (anche in questo caso il tipo pagamento richiesto comprende la ricarica di carte prepagate o il trasferimento di denaro) si ricevono **biglietti assolutamente falsi dotati di codici a barre contraffatti oppure** si tratta di vere e proprie **copie duplicate di biglietti legittimi**.

Anche in questo caso, **valgono semplici, ma importanti consigli pratici**:

1. non fidarsi assolutamente dell'offerta vantaggiosa ed esclusiva, e non cliccare sul link o sul banner promozionale;
2. qualora sia stato difficile resistere e si avesse avuto accesso alla pagina Web, analizzare attentamente l'url del sito, verificare che il sito riporti in calce tutti i dati istituzionali del rivenditore di biglietti, e che siano indicate in maniera trasparente le modalità di pagamento;
3. diffidare da tipologie di pagamento quali ricarica di carte di prepagate e trasferimento di denaro.

La frode del vaglia postale - Postamat

Meglio nota come *frode del postamat*, ha recentemente colpito un incredibile numero di malcapitati, proprio per la modalità particolarmente subdola, e articolata, con cui si concretizza. La vittima, in questo caso, non è un acquirente, ma un venditore (tipicamente di un proprio bene); Il raggiro del Postamat si può sintetizzare nei seguenti passi:

- il venditore (la vittima) mette in vendita su Internet un determinato bene (ad es. un vecchio mobile, un cellulare, una bicicletta o perfino un'automobile);
- l'acquirente (il truffatore) contatta il venditore mostrandosi interessato all'acquisto e propone di effettuare il pagamento attraverso **vaglia postale online**;
- il venditore risponde all'acquirente di non avere un conto corrente postale, ma viene rassicurato da quest'ultimo che non è neces-

sario e che **basta avere un bancomat o una carta di credito** e che è sufficiente **recarsi presso un qualsiasi sportello ATM** (**Postamat**). Il truffatore rassicura inoltre il venditore che lo guiderà telefonicamente per tutta l'operazione, indicando le azioni da eseguire. In questo modo **riceverà più in fretta i soldi spettanti** per la vendita del suo bene.

- A questo punto, molto probabilmente, il venditore si sente rincuorato e procede tranquillo verso il Postamat più vicino per concludere la vendita. Una volta inserito il bancomat o la carta di credito, il falso acquirente guida la vittima passo passo nelle operazioni da eseguire, **suggerendo i pulsanti da cliccare sullo schermo**, **indicando di inserire l'importo pattuito** e **dettando** il **codice** di quello che **dovrebbe essere il vaglia online** che il venditore spera di incassare. Il tutto avviene telefonicamente, senza che ci sia alcuna traccia scritta.
- Se durante l'operazione il venditore solleva dubbi o perplessità, tipicamente il truffatore sarà pronto a tranquillizzarlo e a ripetere che solo facendo così potrà ottenere immediatamente i soldi della transazione, poiché saranno inviati direttamente sulla carta di credito o bancomat utilizzati al Postamat.
- La vittima, fidandosi del premuroso acquirente, completa quindi la procedura (ignorando gli avvisi sullo schermo del Postamat). Purtroppo però, anziché ricevere il denaro pattuito, l'importo è appena uscito dal suo conto corrente per finire sulla carta PostePay del truffatore (carta il cui numero è stato dettato durante la telefonata come numero del vaglia online).

Una **variante della truffa** consiste nel fingere che il pagamento non sia andato a buon fine e quindi il falso acquirente indicherà al malcapitato venditore di **effettuare ripetutamente le operazioni** (così in pratica avvengono **più ricariche di fila della PostePay del malvivente**).
Da segnalare **ulteriori effetti collaterali di questa truffa**: molto spesso il finto compratore invia via WhatsApp copia di documenti personali, quali carta d'identità o codice fiscale, chiedendo altrettanto al venditore. In questo modo il truffatore effettua un **furto di identità del malcapitato**: potrà utilizzare i documenti appena ricevuti per **attivare una SIM** telefonica, con la quale telefonerà e **comunicherà** con le **future vittime**, senza contare che potrà aprire un conto corrente dove farsi accreditare il denaro per i finti acquisti.

Romantic scam - la truffa sentimentale

Tra le truffe più infide messe a segno dai malfattori informatici non si può non citare la truffa romantica, che di romantico non ha proprio nulla: si definisce in questo modo perché fa leva sul bisogno di amore delle persone più fragili. Tutto inizia da una semplice richiesta di amicizia inviata sui social dal profilo di uno sconosciuto, ma è solo l'inizio di un raggiro amoroso che può durare anche svariati mesi, ed ecco perché può essere difficile rendersi conto di essere vittima di una vera e propria truffa, e non protagonisti di una storia d'amore da favola.

La vittima è generalmente una donna sola, di età compresa tra i 40 e i 60 anni, spesso con figli, vedova o divorziata. Il truffatore crea un falso profilo su un Social Network o su una chat room, tipicamente di alto profilo: si tratta quasi sempre di professionisti di successo, imprenditori, architetti, a loro volta vedovi con figli. Lo scopo finale del malfattore è l'estorsione di un'importante somma di denaro. Ma come agisce?

Il suo è un lavoro paziente, lento e psicologico: la vittima, che riceve quotidianamente le sue attenzioni, diventa piano piano dipendente dal falso corteggiatore. Nel momento in cui il truffatore è riuscito a garantirsi la fiducia totale della vittima, teoricamente ci si aspetterebbe un appuntamento dal vivo. E invece no: è in questa fase che accade un qualche tipo di evento drammatico (malattie incurabili, rapimenti, perdita di carte di credito, catastrofi economiche, ecc.). Ovviamente, per uscire da questa situazione, è necessario che la vittima versi immediatamente un'ingente somma di denaro pur di salvare l'amato nei guai. Ovviamente, dopo aver ricevuto il denaro, il finto innamorato sparisce.

Inoltre, il raggiro può facilmente assumere i contorni dell'estorsione se tra la vittima e il malvivente c'è stato lo scambio di foto o video hot e la richiesta di denaro è accompagnata dalla minaccia di diffondere in Rete il materiale se non viene immediatamente pagato un riscatto.

La vittima, dopo essersi resa conto di essere caduta nella trappola, può cadere in una profonda depressione da cui è difficile rialzarsi in quanto è stata tradita la fiducia nell'ambito di quello che sembrava essere un rapporto di vero amore.
Il primo passo per prevenire questa truffa online è l'**informazione**: la consapevolezza che questi truffatori esistono e che, qualora si dovesse cadere nella loro trappola, è fondamentale **sporgere denuncia alla Polizia Postale**, senza vergogna. Inoltre, per aiutare le autorità è importante mantenere traccia delle conversazioni e degli eventuali pagamenti già effettuati.

Decalogo antitruffa: consigli generali per tutelarsi da phishing e scammer online e su dispositivi mobili

1. **Non cliccare mai su link sospetti** e verificare sempre l'URL del sito contenuto nella e-mail: anche se molto simile a siti Web ufficiali, si diversifica per poche parole o caratteri.
2. **Non iscriversi** a siti Web sconosciuti con il proprio indirizzo e-mail
3. **Verificare l'affidabilità del sito Web** su cui si vogliono effettuare acquisti o vendite: se poco noto, cercare recensioni e feedback di altri utenti, e verificare la presenza di certificati di sicurezza, come ad es. VeriSign Trusted che permettono di validarne l'affidabilità.

4. **Se non si è** del tutto **certi** dell'affidabilità della pagina Web **non compilare form** con i propri dati personali.
5. Non effettuare **mai pagamenti** sotto forma di **ricariche** di carte prepagate o servizi di **trasferimento di denaro.**
6. **Non inviare** in nessun caso **scansione di documenti personali** come carta di identità e codice fiscale **via WhatsApp** nè tantomeno ad e-mail sospette.
7. Quando si accede alla rete da un pc desktop, utilizzare **software affidabile** in grado di **bloccare messaggi sospetti e pagine di phishing**, provvedendo a mantenerli **aggiornati** costantemente.
8. Attivare l'**autenticazione a due fattori** (oltre alla password vie-

ne richiesto un ulteriore livello di sicurezza, come ad esempio un codice inviato al proprio numero di cellulare, necessario per procedere con l'autenticazione) **sia sull'account e-mail**, sia sulle applicazioni mobili dei social.

9. **Non digitare mai le credenziali** per accedere agli account dei propri Social Network **su servizi e app di autenticazione di terze parti**.
10. Utilizzare sempre le **versioni aggiornate** delle **applicazioni** di Social Network e Instant Messaging **scaricate** dagli **store ufficial**i Google Play per Android e App Store di iOS.

Fonti

- *https://wearesocial.com/it/blog/2019/01/digital-in-2019*
- *http://www.prefettura.it/sondrio/contenuti/Difendersi_dalle_trappole_dell_e_commerce_i_10_consigli_del_ministero_dell_interno-7583987.htm*
- *https://www.mobileworld.it/2018/02/01/whatsapp-utenti-attivi-2017-143496*
- *https://tecnologia.libero.it/whatsapp-il-nuovo-pericolosissimo-gioco-che-spopola-tra-i-giovani-29376*
- *https://www.cybersecurity360.it/nuove-minacce/truffe-on-line-dal-furto-di-denaro-al-furto-di-identita24818/*
- *https://it.businessinsider.com/le-11-truffe-online-piu-sofisticate-in-giro-in-questo-momento-occhio-a-non-cascarci/amp/*
- *https://www.corrierecomunicazioni.it/cyber-security/truffa-instagram/*
- *https://questure.poliziadistato.it/it/Gorizia/articolo/7665c1238911c028572437816*
- *https://www.romantic-scam.eu*
- *https://sociologicamente.it/romance-scam-le-truffe-sentimentali-online-laltra-faccia-del-cybercrime/*

FORME DI PAGAMENTO SICURO

Dopo queste premesse, c'è da chiedersi come sia possibile fidarsi dei pagamenti online. Eppure i dati parlano chiaro: i pagamenti digitali su e-commerce in Italia valgono complessivamente diversi miliardi di euro. Quindi, è bene saper identificare quali sono i possibili indicatori che garantiscono la sicurezza della transazione. In questa sezione sono riportate le forme di pagamento classiche proposte dai siti di e-commerce e vengono illustrati i più recenti canali di pagamento sicuri.

Le forme di pagamento classiche

Comunemente un rivenditore online permette di effettuare il pagamento dei beni o servizi acquistati tramite:

- **Contrassegno**: questa modalità prevede il pagamento della merce al momento della sua ricezione, direttamente al corriere. Per il proprietario dell'e-commerce può risultare più rischioso, ma agevola l'acquisto per chi ha scarsa fiducia nell'utilizzare i pagamenti online. Solitamente l'esercente applica al prezzo finale della merce, un ricarico per il contrassegno di qualche euro.
- **Bonifico bancario**: se il bonifico bancario è tradizionale, e non istantaneo (possibilità che dipende principalmente dalle tipologie di servizi offerti dall'Istituto di credito sulla base del proprio conto corrente) l'evasione dell'ordine non è mai contestuale al pagamento, ma avviene al momento dell'accredito sul conto corrente bancario dell'esercente, sulla base dei giorni di evasione del bonifico tra banche.

- **Carta di credito**: il cliente inserisce nome e cognome (intestatario della carta), il codice numerico della carta di credito, la data di scadenza, il codice di sicurezza e successivamente viene reindirizzato ad un cosiddetto ***gateway di pagamento.*** Cosa succede quindi esattamente tra il momento in cui il cliente inserisce il numero della propria carta di credito e il momento in cui l'esercente riceve pagamento? Il modo con cui gli acquisti vengono processati dipende dal canale di pagamento.

CANALI O GATEWAY DI PAGAMENTO

Si tratta di intermediari 'virtuali', che dopo aver ricevuto le informazioni inserite sull'e-commerce, le processano facilitando l'autorizzazione o l'esecuzione dei pagamenti effettuati ad un e-commerce.
Le funzionalità di un gateway di pagamento sono:
- la **criptazione dei dati sensibili** dell'utente, come numero di carta di credito e codice di sicurezza;
- il **rispetto di determinati standard** a garanzia della sicurezza dei dati e delle transazioni tra utente e negozio virtuale;
- offrire **flessibilità nei tipi di pagamento** che i clienti possono utilizzare.

Tali caratteristiche permettono di approcciarsi con maggiore sicurezza e confidenza al pagamento dei propri acquisti online.

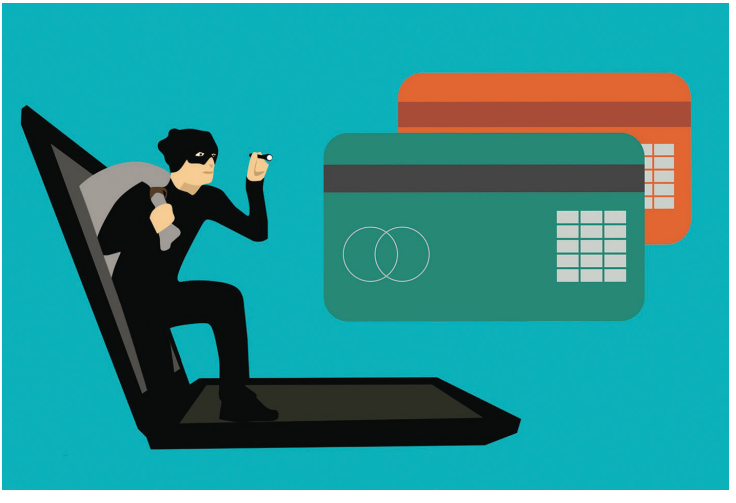
I 10 gateway di pagamento più utilizzati per permettere acquisti online sicuri

È bene che il sito di e-commerce su cui si stanno per effettuare acquisti riporti almeno uno dei seguenti loghi.

Si tratta proprio dei cosiddetti gateway di pagamento; di seguito si riportano le caratteristiche essenziali dei **10 gateway** ad oggi più utilizzati dagli e-commerce italiani:

1. **Gateway Banca Sella - gestpay Banca Sella** - è il gateway più utilizzato in Italia e permette di effettuare gli acquisti attraverso le principali carte di credito, con Paypal e con MyBank; permette di abilitare i sistemi di sicurezza Verified by Visa e Mastercard Secure Code e di effettuare il controllo dei CVV e 4DBC.
2. **MonetaWeb 2.0** di Mercury Payment System (ex Setefi MonetaWeb - Banca Intesa Sanpaolo) - è un POS virtuale di ultima generazione che gestisce i pagamenti online attraverso i principali circuiti internazionali garantendo il rispetto degli standard di sicurezza definiti dai circuiti internazionali quali Verified by Visa e Mastercard Secure Code; la trasmissione dei dati sensibili è crittografata secondo il protocollo HTTPS.
3. **Amazon Payments** - offre agli acquirenti un modo semplice e conosciuto per effettuare gli acquisti; disponibile su tutti i dispositivi e perfettamente funzionante anche su smartphone e tablet, a livello mondiale i clienti che utilizzano Amazon Pay hanno superato i 33 milioni.
4. **Paypal -** considerato un veterano del commercio elettronico, è uno dei metodi di pagamento più accettati e richiesti. L'utente una volta cliccato sul pulsante *Acquista*, viene reindirizzato sul server sicuro Paypal.
5. **Wepay** - è in grado di gestire richieste di pagamento complesse, come ad esempio molteplici pagatori o campagne di crowdfunding, e funziona su siti di diverse dimensioni.
6. **Authorized.net -** garantisce un'esperienza di acquisto decisamente positiva grazie a un sigillo di sicurezza verificato e pagine di pagamento personalizzate. È dotato inoltre di un pacchetto anti-frode avanzato, che offre un servizio di sicurezza gratuito.
7. **Stripe** - processore di pagamenti di terze parti offre transazioni altamente sicure: grazie a integrazioni con reti di carte come Visa, MasterCard e American Express, è in grado di accelerare il processo e migliorare il successo delle transazioni. Aggiunge inoltre un ulteriore livello di autenticazione per evitare rischi di frode e clonazione di carte. Anche la gestione delle controversie è automatizzata per presentare in modo efficiente le prove in caso di contenzioso; supporta inoltre i portafogli digitali come Alipay, Amex Express Checkout e Apple Pay.

8. **MyBank** - piattaforma che consente di effettuare in modo sicuro pagamenti online utilizzando il servizio di *online banking* della propria banca all'interno del sito di e-commerce: grazie a un collegamento tra il conto corrente bancario del cliente e la banca dell'esercente, MyBank evita la richiesta e la memorizzazione di dati personali. Permette inoltre di effettuare bonifici immediati e irrevocabili, sfruttando i reciproci vantaggi offerti da una carta di credito e da un bonifico bancario.
9. **2Checkout** - questo gateway consente all'acquirente di utilizzare diversi metodi di pagamento come carte di credito, carte di debito e PayPal, utilizza una sofisticata protezione antifrode basata su centinaia di controlli oltre ad essere certificata PC1 - è il livello più alto che un'azienda possa avere.
10. **POS virtuale – Poste Italiane** - oltre a interagire con conto BancoPosta e le carte prepagate Postepay permette il pagamento tramite carte di credito appartenenti ai circuiti internazionali Visa, Visa Electron e MasterCard, garantendo i protocolli di sicurezza elevati con "Verified by Visa" e "MasterCard Secure Code".



5 passi da seguire per assicurarsi di effettuare pagamenti su siti di e-commerce sicuri

1. Innanzitutto **effettuare acquisti** solo su siti di **e-commerce con connessione protetta** (l'indirizzo del sito deve iniziare con **https**);
2. **Cercare informazioni** circa l'**affidabilità del venditore** attraverso, ad esempio, recensioni su portali come TrustPilot;
3. **Leggere** con molta attenzione le **condizioni generali di vendita** anche se ti sembra di perdere tempo con un'attività noiosa: non cliccare su caselle di accettazione senza conoscere le informazioni per i tuoi acquisti;

4. **Verificare la completezza** e la trasparenza delle informazioni presenti sull'e-commerce, accertando che siano riportati tutti i dettagli del negozio online: controllare quali sono le modalità di pagamento (verificando quali sono i gateway di pagamento, le condizioni di recesso, la pec per i reclami, ecc.);
5. **Controllare sempre la descrizione** di un prodotto, facendo **attenzione a offerte super convenienti** così come a richieste di pagamenti online anticipati.

Fonti

- *http://www.cartedipagamento.com/merchant/gestpay.htm*
- *https://www.soisy.it/pagamenti-online-in-sicurezza/*
- *https://www.ecommerce-nation.it/piattaforme-pagamento-elettronico-ecommerce/*
- *https://www.alground.com/site/sistemi-pagamento-ecommerce/53756/*
- *https://ecommerce-platforms.com/it/ecommerce-selling-advice/choose-payment-gateway-ecommerce-store*
- *https://www.nethics.it/metodi-di-pagamento-nelle-commerce/*

ADESCAMENTO ONLINE DI MINORENNI

L'adescamento online di minorenni è un fenomeno criminale vero e proprio, una piaga sociale del nuovo millennio, facilitata dalla totale libertà e facilità di accesso dei giovanissimi a giochi online, a Social Network, ad applicazioni di instant messaging, a siti e applicazioni di incontri per ragazzi, per affrontare i quali servirebbe una maggiore consapevolezza sui reali pericoli che si possono incorrere nella Rete e la dovuta formazione in materia di privacy.

Uno studio condotto da Ecpat (End Child Prostitution, Pornography and Trafficking) su un centinaio di studenti di 13 anni, ha evidenziato che il 90% di essi ha creato un profilo Facebook prima del limite minimo di 13 anni e l'80% di questi giovani utenti condivide un post con una foto al giorno dove, se compaiono conoscenti, non viene chiesta alcuna autorizzazione. Il 60% ha ricevuto richieste a sfondo sessuale e il 90%, in caso di pericolo online, teme principalmente la reazione dei genitori ai quali, di conseguenza, non ne parla. Save the Children, in una recente indagine riporta che 1 teenager su 3 dà il numero di cellulare a persone conosciute online. Questi dati dimostrano l'esigenza di affrontare una vera e propria emergenza in termini di sicurezza dei minori online.

L'adescamento, in inglese definito come ***child grooming*** (dal verbo *to groom*, prendersi cura) è definito come il "*tentativo da parte di un adulto di avvicinare un bambino/a o un adolescente per scopi sessuali, conquistandone la fiducia al fine di superare le resistenze emotive ed instaurare con lui/lei una relazione intima o sessualizzata*".

In Italia è un reato dal 2012 definito come "*qualsiasi atto volto a carpire*

la fiducia di un minore di anni sedici per scopi sessuali, attraverso artifici, lusinghe o minacce posti in essere anche mediante internet o altre reti o mezzi di comunicazione". È importante precisare che il reato si configura anche se l'incontro nel mondo reale con il minore non avviene: pertanto, se l'adescamento non va a buon fine, è sufficiente il tentativo affinché il reato sussista.
Questo tipo di criminale si presenta ai giovanissimi come confidente premuroso, particolarmente attento ai bisogni e ai desideri del minore: come riconoscere quindi un tentativo di adescamento? Di seguito vengono riportate le fasi più comuni messe in atto per adescare un minorenne.

Modalità di adescamento

Una recente indagine Audiweb ha registrato l'accesso alla Rete da parte dei giovani e giovanissimi attraverso l'uso del computer: il 3% di bambini tra i 2 e 10 anni naviga liberamente in Internet almeno mezz'ora al giorno; per i ragazzi tra 10 e 17 anni la percentuale sale al 7,5% così come aumenta di media il tempo utilizzato giocando online.

Sempre più spesso lo scenario in cui l'adescatore muove i suoi passi sono le **chat di videogiochi online**: in generale lo scopo principale del delinquente consiste nel garantirsi innanzitutto la fiducia della vittima, mostrandosi come migliore amico di cui fidarsi ciecamente, per poi spostarsi su altre piattaforme di messaggistica privata (Messenger, Skype, WhatsApp). Su queste chat i contenuti sessuali diventano espliciti: qui l'adescatore **richiede video o foto di nudo in cambio di ricariche utili all'acquisto di aggiornamenti del gioco**.
Le statistiche mostrano che il comportamento dell'adescatore segue un copione sintetizzabile in 5 fasi:

1. **Fase dell'amicizia iniziale** - *Friendship Forming Stage (FFS)*
   Il *groomer*, nascosto dietro a un nickname scelto appositamente per

attirare l'attenzione della propria vittima osservata all'interno dell'ambiente virtuale (Social Network o videogioco che sia) instaura un primo contatto e di solito richiede l'invio di una fotografia o l'attivazione di una webcam per verificare l'età della giovane vittima.

2. **Fase della costruzione del rapporto di fiducia** - *Relationship Forming Stage (RFS)*
   L'adescatore cerca di ottenere gradualmente la fiducia della vittima, spacciandosi per "migliore amico": condivide interessi, bisogni e stati d'animo della preda, ponendogli/le la massima attenzione.
3. **Fase di valutazione del rischio** - *Risk Assessement Stage (RAS)*
   L'adescatore testa il livello di privacy nel quale si svolge l'interazione con il bambino, per comprendere se può spostare la relazione da un contesto virtuale ad uno contesto reale. È questa la fase critica dell'adescamento: il predatore, da *internet offender* (offensiva solo sul piano virtuale) diventa un *contact offender* (un pericolo reale e concreto per la vittima).
4. **Fase dell'esclusività -** *Esclusivity Stage (ES)*
   L'adescatore rende isolato il minore facendo leva sulla segretezza della loro relazione e tagliandolo fuori dai punti di riferimento (genitori, ma più spesso altri amici). Questo è un approccio più intimo che conduce velocemente alla relazione sessuale; il groomer continuerà a utilizzare frasi, atteggiamenti e videochat convincendo la vittima di essere l'unica persona che può capirlo e soddisfarlo.
5. **Fase della relazione sessualizzata** - *Sexual Stage (SS)*
   L'adescatore fa di tutto per rendere la situazione "normale" agli occhi del minore, al fine di superare le sue ultime resistenze. Superate le quali, l'abuso può consumarsi attraverso:
   • un incontro personale che può sfociare in una violenza sessuale;
   • virtualmente tramite lo scambio di materiale pedopornografico o l'interazione via webcam o live streaming.

Una volta comprese le dinamiche del ***child grooming*** la strategia migliore è formare sia i giovani che i loro genitori sui comportamenti da seguire quando si interagisce su piattaforme online e nello specifico sulle azioni da fare (e spesso non fare) per evitare di cadere nelle trappole di questi predatori senza scrupoli.

Vademecum ragazzi

- Non divulgare alcuna informazione su di te, sulla tua famiglia o sui tuoi amici in nessun caso, se non sotto la supervisione di un adulto;
- Non inviare foto o video personali a persone che hai conosciuto in rete, ricorda: una volta finiti online non sono più eliminabili dalla Rete e se ne perde completamente il controllo;
- Non credere mai alle apparenze: è facile mentire on-line, le persone che si incontrano online non sono sempre quelle che dicono di essere e possono nascondere le vere intenzioni per cui ti vogliono contattare. Le informazioni che conosci su questa persona potrebbero essere completamente false.
- Non incontrare mai qualcuno conosciuto solo tramite la Rete, anche se sono state inviate sue foto o se la persona si è vista attraverso una webcam: le immagini possono essere modificate;
- Non divulgare mai a nessuno le tue password, nemmeno ai tuoi amici: si tratta di una informazione personale riservata;
- Se qualcuno si rivolge a te in una chat e ti mette in imbarazzo, o ti spaventa, o ti propone azioni che ritieni strane, ambigue e che i tuoi genitori hanno detto di non compiere, blocca immediatamente il contatto. Nessuno ti può obbligare a continuare una conversazione online o a fare qualcosa che non vuoi;
- Appena qualcosa mette a disagio, o se un contatto conosciuto online ti chiede di incontrarlo di persona, parlane subito con i tuoi genitori o con i tuoi insegnanti. Non devi avere paura di una eventuale punizione o non devi vergognarti: tu non hai nessuna colpa e anzi, grazie alla tua azione, potresti aiutare altri giovani come te che possono finire in situazioni pericolose con quegli stessi contatti.

Vademecum genitori

Il genitore che sospetta o ha la certezza che un minore sia coinvolto in una situazione rischiosa deve tempestivamente rivolgersi alla Polizia Postale e delle Comunicazioni. È altrettanto importante non sostituirsi al minore stesso, rispondendo ad esempio al suo posto all'adescatore, ma tenere traccia delle conversazioni (facendo degli screenshot e salvando più informazioni possibili). Ciò può facilitare il lavoro di indagine e potrebbe aiutare a prevenire al contempo anche altre situazioni a rischio. *Di seguito il vademecum dedicato ai genitori*

1. Fate voi stessi esperienza diretta di navigazione in Internet: senza un minimo di cultura informatica, non è possibile conoscere e di conseguenza utilizzare appositi strumenti di difesa e di controllo.
2. In caso di bambini più piccoli, usate dei software di protezione (o filtri) per monitorare l'uso di Internet.
3. Controllate periodicamente la "cronologia" dei siti Web utilizzando gli appositi strumenti del browser.
4. Installate e fate usare ai vostri figli più piccoli browser Web appositamente creati per loro (ad es. *Kidzy* è un **browser Web** gratuito, creato appositamente **per i bambini** in quanto offre una navigazione in un ambiente sicuro e protetto mettendo a disposizione degli adulti funzioni di *parental control*).
5. Scrivete assieme ai bambini più piccoli le regole di comportamento da appendere accanto al computer.
6. Controllate l'uso del pc da parte dei più piccoli, posizionandolo in uno spazio comune all'interno della casa.
7. Interessatevi a cosa fanno i vostri figli online e dialogate con loro, spiegando in modo semplice le potenzialità della Rete (ad esempio com'è semplice fare una ricerca di scienze) e i rischi, che derivano dalle persone e non dallo strumento di per sé. Parlate apertamente del rischio di imbattersi durante la navigazione in potenziali malintenzionati: rassicurateli che non devono vergognarsi a chiedervi informazioni sull'argomento o a confidarvi eventuali "brutti incontri online"
8. Non fornite dati personali (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici, ma anche indirizzo e-mail) che possono rendere i bambini e i ragazzi facilmente individuabili e raggiungibili.
9. Insegnate ai vostri ragazzi a utilizzare correttamente le impostazioni sulla privacy dei vari Social Network e a bloccare quei contatti che li infastidiscono online

Fonti:

- https://www.ecpat.org/
- https://www.cyberlaws.it/2019/adescamento-minori-child-grooming/
- https://www.lastampa.it/cultura/2018/04/27/news/quanti-minorenni-usano-i-social-network-1.34010836
- https://d.repubblica.it/attualita/2014/06/09/news/web_minori_social_network_adescamento-2173056/
- https://www.triesteallnews.it/2019/02/10/cadere-nella-rete-di-internet-389-i-reati-a-danni-di-minori/
- https://terredeshommes.it/comunicati/presentato-il-dossier-indifesa-2018/
- https://www.generazioniconnesse.it/site/it/adescamento-scuole/

Contatti utili

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA
Piazza Oberdan, 6
34133 Trieste
Tel. 0432. 555708
garantefvg@regione.fvg.it
http://www.consiglio.regione.fvg.it/cms/pagine/garante-diritti-per-so- na/bambini/
Competenze/Servizi: segnala all'autorità giudiziaria i servizi sociali competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

POLIZIA POSTALE E DELLE COMUNICAZIONI
Compartimento di Trieste
Piazza Vittorio Veneto n. 1, 34100
Tel. 040. 6764589
poltel.ts@poliziadistato.it
www.commissariatodips.it/
Competenze/Servizi: accoglie tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di Internet e che si configurano come reati.
Tipologie di comportamenti che configurano un reato: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line nel caso di clonazione di carta di credito, pedopornografia on-line, *grooming* (adescamento on-line), gioco d'azzardo on-line, *sexting*.

Federconsumatori
Friuli Venezia Giulia

www.federconsumatori-fvg.it *www.cittadinoconsumatore.it*

Federconsumatori FVG

SEDE LEGALE REGIONALE
Borgo Aquileia 3/B
33057 PALMANOVA (UD)
tel. 0432 935548
admin@federconsumatori-fvg.it

SEDE OPERATIVA REGIONALE
Via Torino, 64
33100 UDINE
tel. 0432 935548
admin@federconsumatori-fvg.it

SEDI DELLE STRUTTURE PROVINCIALI

TRIESTE
Via Matteotti, 3 (angolo via Manzoni)
34138 TRIESTE
tel. 040 773190
trieste@federconsumatori-fvg.it

UDINE
Via Mantova, 108/B
33100 UDINE
tel. 0432 45673
udine@federconsumatori-fvg.it

GORIZIA
Via XXV Aprile, 48
34074 MONFALCONE (GO)
tel. 0481 790434
monfalcone@federconsumatori-fvg.it

PORDENONE
Via San Valentino, 20/A
33170 PORDENONE
tel. 0434 247175
pordenone@federconsumatori-fvg.it

2019 © Federconsumatori Friuli Venezia Giulia
Riproduzione vietata a fini commerciali
Realizzazione grafica e stampa a cura di: Cronaca Fvg s.a.s

Inserto di Cittadino Consumatore n. 59

REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

Realizzato con i fondi della LR 16/2004 - programma 2018