

Report di indagine

SCOVA la truffa



Progetto realizzato nell'ambito di Noi&UniCredit, il programma di partnership fra la banca e le Associazioni Consumatori di rilevanza nazionale a cui Adiconsum partecipa attivamente dal 2005.

ADICONSUM
Associazione Difesa Consumatori APS
dal 1987

www.adiconsum.it

Indice

1. Introduzione	P.2
2. Il quiz e i profili	P.3
3. I dati demografici	P.4
4. Le risposte	P.5
5. Principali evidenze	P.10

Introduzione

Il **mondo digitale**, con la sua innegabile comodità e le infinite opportunità che offre, nasconde anche un lato oscuro sempre più insidioso: **le truffe online**. Dalle più comuni e-mail di **phishing**, che tentano di carpire dati personali e credenziali bancarie, alle sofisticate frodi che sfruttano **l'intelligenza artificiale** per creare scenari ingannevoli, gli italiani sono diventati un bersaglio privilegiato per **hacker e truffatori**. Basta un attimo di distrazione, un clic affrettato, per cadere in una **trappola** ben congegnata e vedere i propri risparmi dissolversi nel nulla.

La gravità di questa situazione è stata recentemente messa in luce da uno studio congiunto di mUp Research e Norstat per facile.it, che ha rivelato un dato estremamente allarmante: quasi **3 milioni di italiani**, per l'esattezza 2,9 milioni, **sono già stati vittime di truffe digitali**. Un numero che sottolinea **l'urgenza di rafforzare la consapevolezza** e la preparazione dei cittadini di fronte a queste **minacce sempre più pervasive**.

In questo contesto di crescente vulnerabilità, **Adiconsum**, nell'ambito del programma **Noi&UniCredit** - il programma di partnership fra la banca e le Associazioni Consumatori di rilevanza nazionale a cui Adiconsum partecipa attivamente dal 2005 - scende in campo con il progetto **"Scova la truffa"**. Questa campagna ha un duplice obiettivo: da un lato, testare il livello di conoscenza dei consumatori italiani rispetto alle tipologie di truffa più diffuse; dall'altro, fornire strumenti concreti e conoscenze pratiche per imparare a difendersi efficacemente.

"Scova la truffa" è un innovativo percorso di infotainment. Non si tratta di una semplice lezione frontale, ma di un'esperienza interattiva e coinvolgente progettata per massimizzare l'apprendimento. Attraverso un sondaggio, i partecipanti hanno avuto l'opportunità di mettere alla prova le proprie conoscenze in materia di sicurezza digitale. Questo approccio ludico-educativo permette non solo di identificare le proprie lacune, ma anche di acquisire in modo intuitivo nuove informazioni su come comportarsi per evitare spiacevoli imprevisti e proteggere i propri beni.

Il questionario è stato ideato per simulare situazioni reali, esponendo i partecipanti a scenari di truffa comuni, dal finto SMS bancario, alle offerte online "troppo belle per essere vere". L'intento è quello di sviluppare un "occhio critico" e una maggiore sensibilità ai segnali d'allarme, trasformando la teoria in pratica quotidiana.

Il quiz e i profili

Il quiz

Il quiz è stato pensato come una simulazione della realtà quotidiana, proponendo gli scenari di truffa più diffusi.

Alla fine del quiz ogni partecipante ha potuto visionare le risposte corrette ed un commento contenente informazioni utili per saperne di più sul tema della domanda.

In questo modo il quiz è diventato anche un'occasione per avere informazioni utili per gestire al meglio eventuali tentativi di frode.

Sono stati ben **716** i cittadini-consumatori che hanno deciso di mettersi alla prova e fare un check up delle proprie abilità investigative.

I profili

Alla fine del questionario, in base alle risposte fornite, ad ogni partecipante è stato attribuito un profilo per rendere l'esperienza più ludica e coinvolgente.

Di seguito i profili:



Gufo Maestoso

Sei curioso e scrupoloso, nel digitale vittorioso!



Volpe Eccellente

Hai un fiuto sorprendente ma attenta, sii prudente!



Rana Curiosa

Ti butti al volo, sei coraggiosa... ma attenta: la truffa è silenziosa

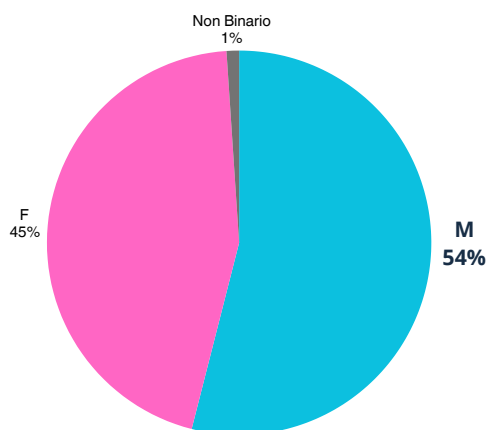


Talpa Insicura

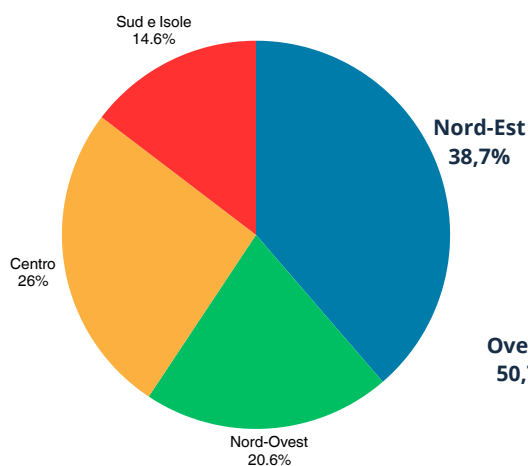
Se non ti informi un pò, in rete sarà dura!

I dati demografici

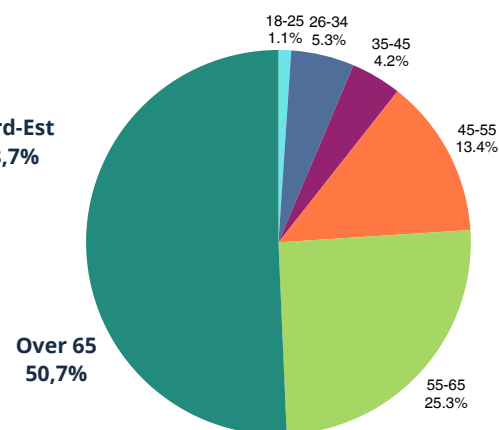
Genere



Area geografica



Età



Titolo di studio



Dottorato / master

9%



Laurea

24%



Diploma

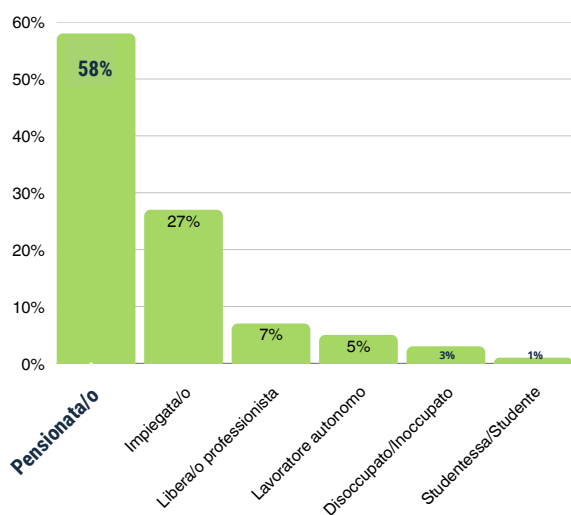
55%



Licenza elementare

12%

Professione



Il profilo medio di chi ha partecipato al sondaggio

Il consumatore medio che ha partecipato all'indagine è un pensionato maschio che ha conseguito il diploma e vive nel nord est

Le risposte

Se dovessi dare un voto alle tue competenze in termini di utilizzo degli strumenti digitali di pagamento e per la gestione del denaro (internet banking, wallet, carte di pagamento digitali, etc.), quale punteggio ti attribuiresti?

53%

Niente male, direi che me la cavo

28%

Sufficiente, conosco questi strumenti ma li utilizzo poche volte al mese

10%

Il massimo

8%

Preferisco fare tutto in banca, la tecnologia non fa per me

1%

Ho l'app ma non la utilizzo, saranno anni che non cambio nemmeno la password

Ricevi un SMS da un numero, che sembra essere quello della tua banca, che ti comunica che il tuo conto è stato bloccato e che riceverai una chiamata da parte di un operatore. Poco dopo arriva la chiamata da parte di un operatore che ti segnala che è possibile sbloccare il conto comunicando dei codici che vedrai comparire sul telefono o nella tua mail. Cosa fai?

63%

Chiudo la chiamata senza fornire informazioni, controllo il mio conto sull' internet banking e contatto la mia filiale o il servizio clienti della banca per segnalare quanto accaduto



19%

Chiudo la chiamata senza fornire informazioni, ma non faccio altri controlli tanto so che si tratta di una truffa

15%

Chiudo la chiamata senza fornire informazioni, poi contattato il mio istituto di credito recandomi presso la mia filiale di riferimento

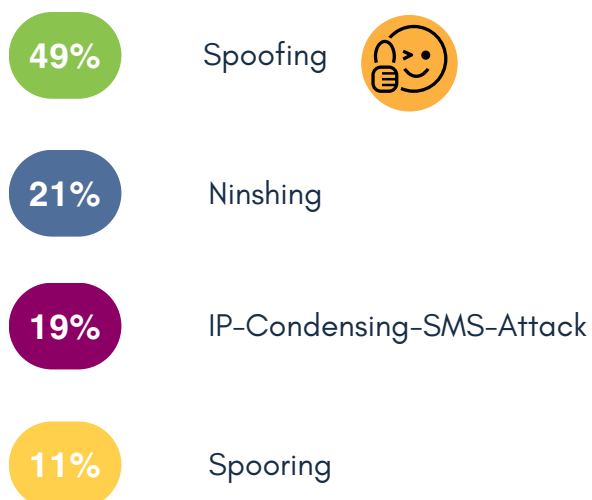
3%

Se il numero è quello della banca non c'è bisogno di preoccuparsi

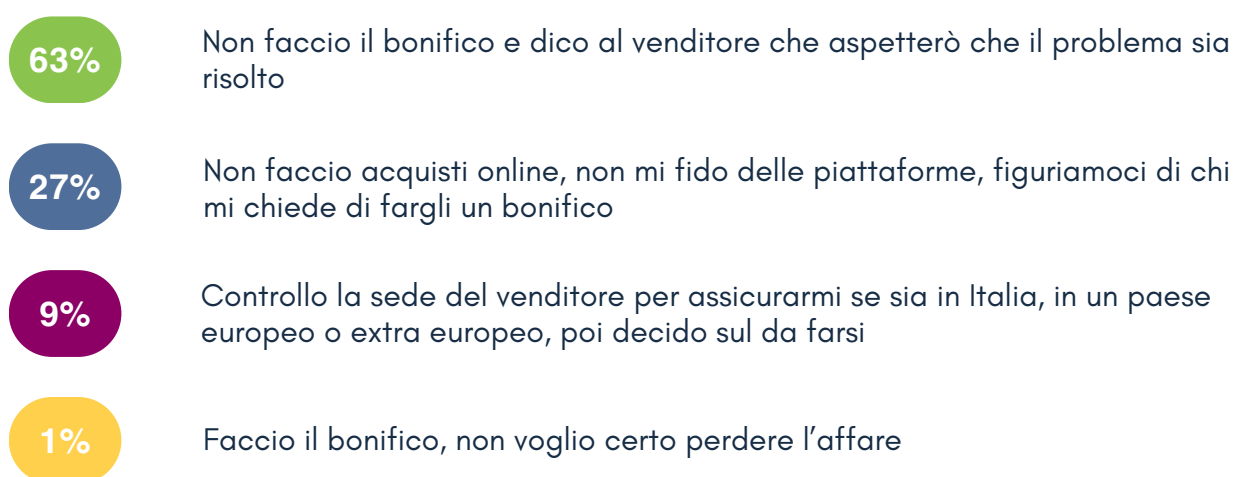


**Indica la risposta più corretta e completa*

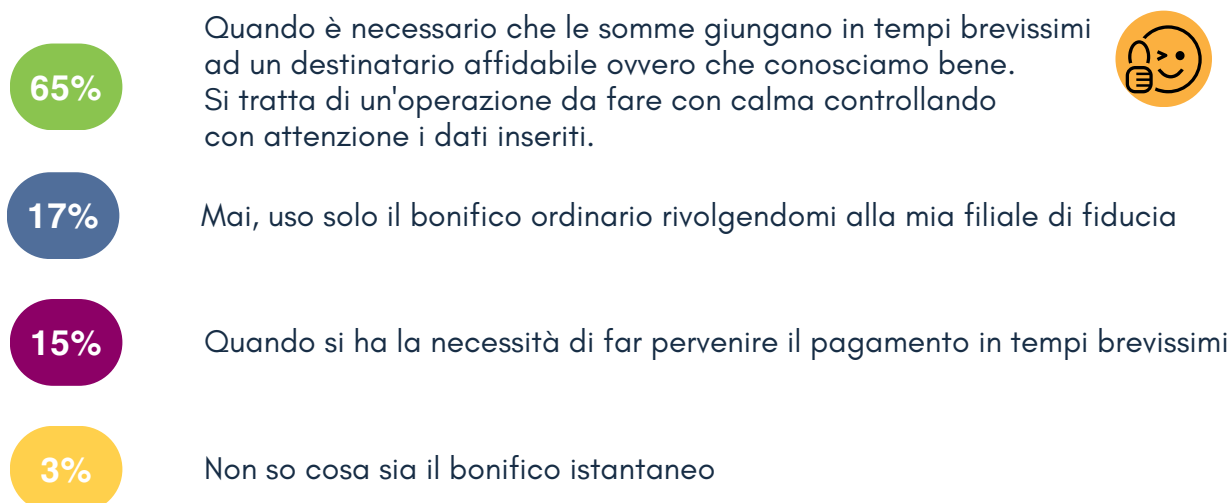
“Attacco informatico che, attraverso la manipolazione della tecnologia voice-ip o altre tecniche, consente ai truffatori di utilizzare numeri riconducibili alla banca avendo così la possibilità di spacciarsi per un operatore del servizio clienti e ottenere dalla vittima designata accesso a informazioni riservate, dati sensibili o sottrarre denaro.” Come si chiama questa truffa?



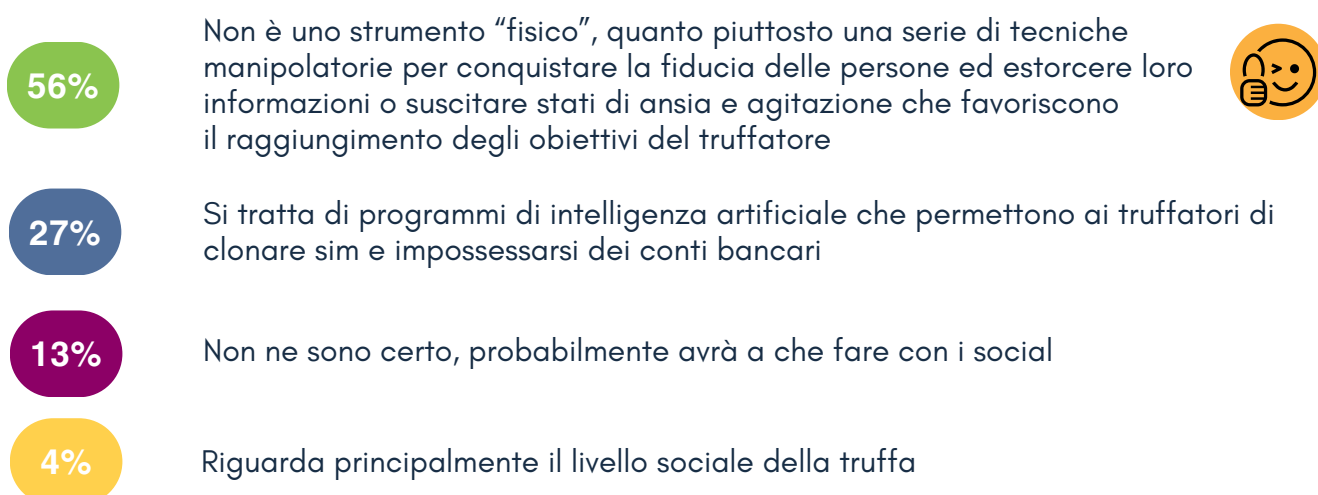
Hai appena acquistato un prodotto attraverso un grande piattaforma di e-commerce; che fortuna, il prodotto che cercavi era disponibile a metà del prezzo di mercato. D'improvviso ricevi dal venditore una mail che ti avvisa che il tuo ordine è stato annullato: c'è un problema con i pagamenti tramite la piattaforma. Ti propone quindi di inviargli un bonifico. Cosa fai?



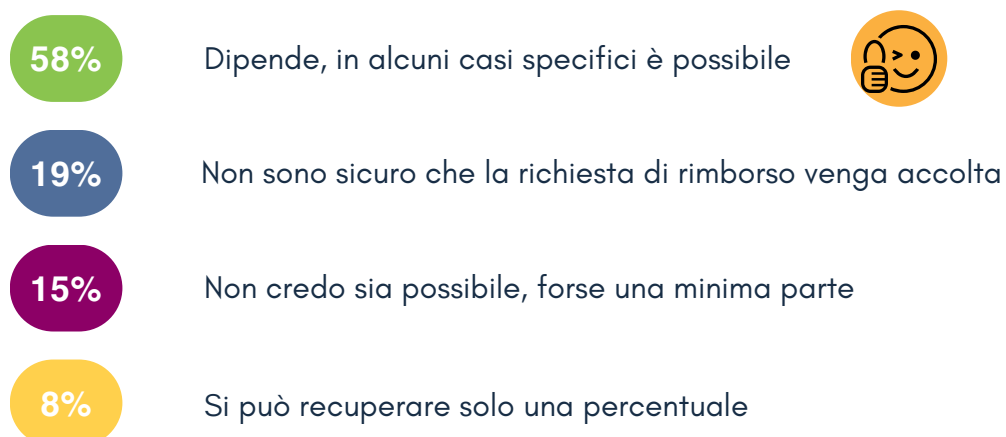
Quando è preferibile utilizzare il bonifico istantaneo?



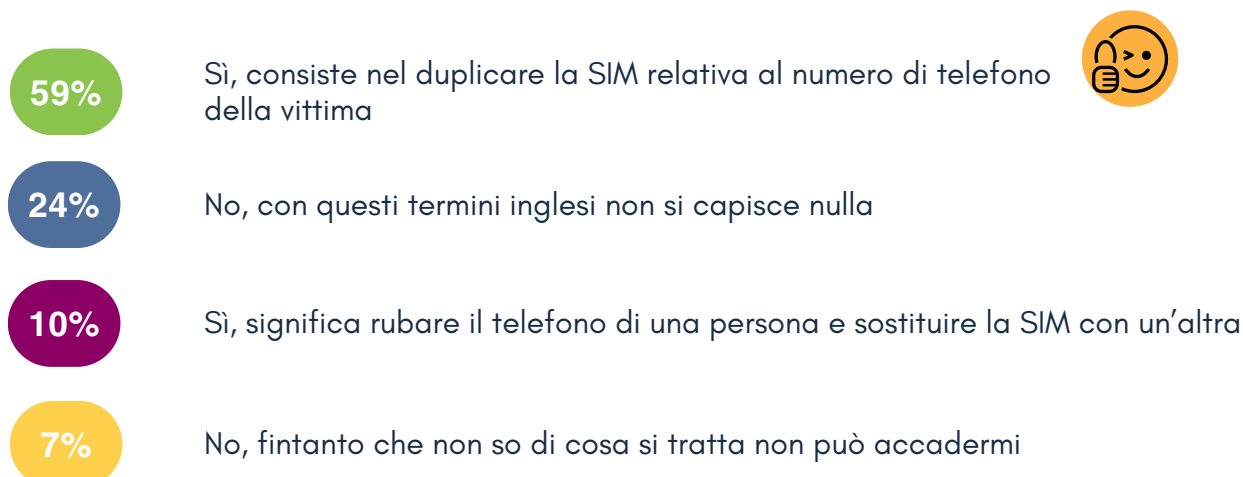
Uno strumento comunemente utilizzato nelle truffe bancarie è l'ingegneria sociale o social engineering, di cosa si tratta?



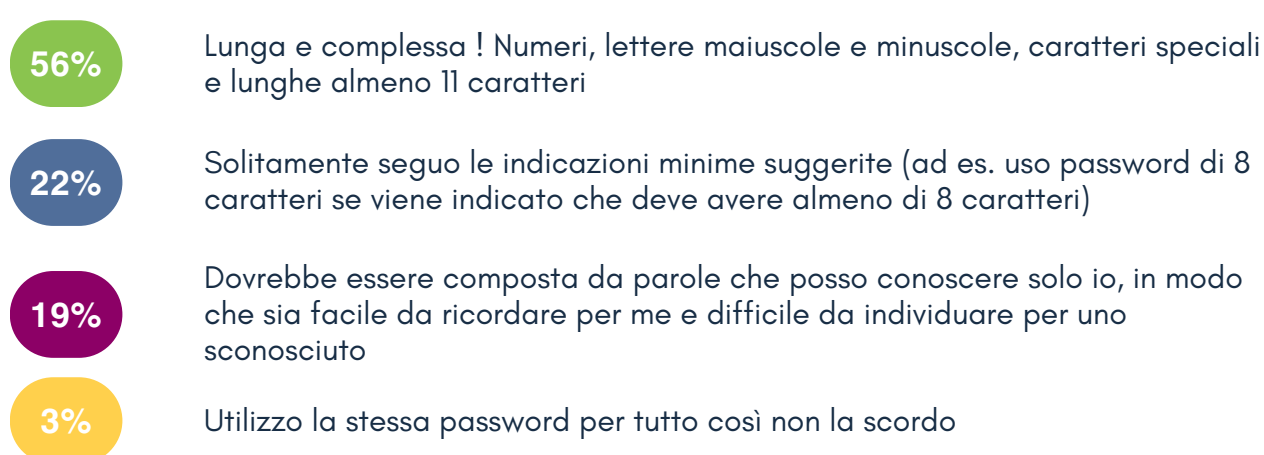
La vittima di una truffa può richiedere di farsi rimborsare il denaro sottratto dai frodatori?



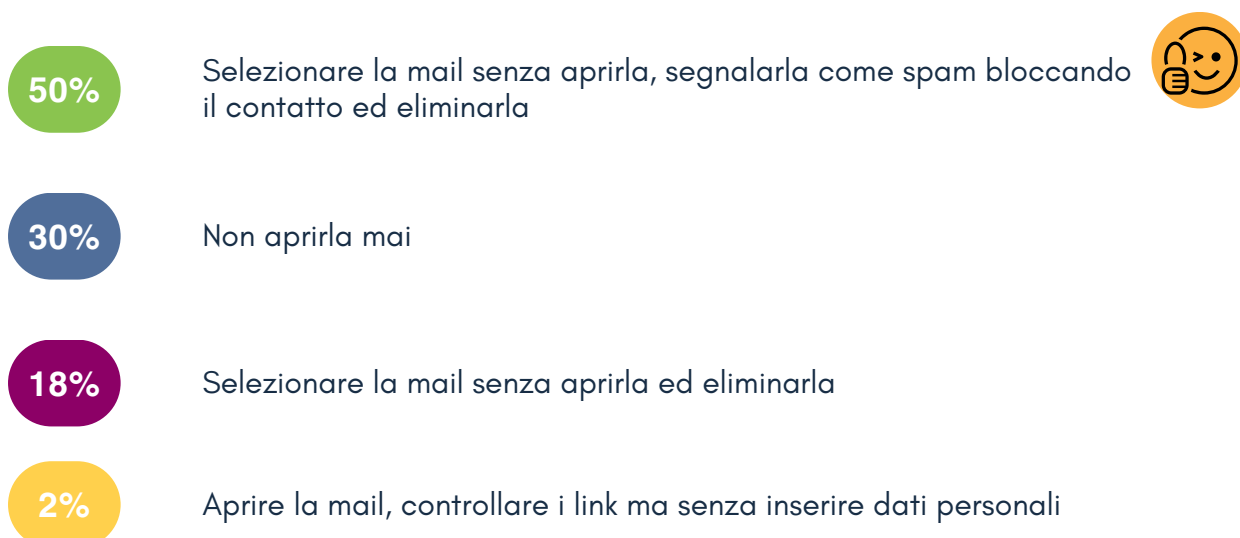
Hai mai sentito parlare di Sim Swap?



Come dovrebbe essere una password efficace?



Il termine phishing è ormai entrato nel gergo comune, spesso queste mail fasulle contenenti link pericolosi vengono intercettate dai filtri antispam, se questo non accadesse la procedura da seguire sarebbe:



Hai buon occhio? Vediamo se riesci a identificare il vero logo di Adiconsum

ADICONSUM
Associazione Difesa Consumatori APS
dal 1987

59%



ADICONSUM
Associazione Difesa Consumatori
dal 1987

17%

ADICONSUM
Associazione Difesa Consumatori APS

14%

ADICONSUM
Associazione Difesa Consumatori APS
dal 1987

10%



Principali evidenze

Analizzando le risposte del quiz emerge che il 76% dei partecipanti ha ottenuto il profilo “Gufo maestoso” che indica una maggioranza di risposte corrette.

Infatti, ad esempio, alla domanda che indaga il comportamento dei consumatori qualora ricevano un SMS da un numero che potrebbe sembrare quello della propria banca e successivamente vengano contattati telefonicamente da un operatore che afferma che per sbloccare il conto sia necessario fornire i codici inviati via sms o via mail, il 97% dei partecipanti afferma che chiude la chiamata senza fornire informazioni ed il 67% contatta anche la propria banca per segnalare l'accaduto. O, ancora, il 65% indica correttamente le caratteristiche del bonifico istantaneo.

A fronte di questi aspetti positivi si rileva:

- una scarsa dimestichezza con i termini inglese utilizzati per indicare alcune tipologie di truffa (spoofing, sim swap, etc.);
- una certa diffidenza verso le piattaforme di acquisto online (il 27% dichiara di non fidarsi di questo canale);
- la scarsa dimestichezza con i bonifici istantanei (il 17% usa solo bonifici ordinari facendoli presso la propria filiale di fiducia e il 3% dichiara di non sapere cosa siano)
- l'adozione di comportamenti che possono esporre a rischi, come ad esempio coloro che utilizzano la stessa password per diversi account (3% degli intervistati).

Segnale che tanto è stato fatto per accrescere la consapevolezza dei consumatori su questi temi di grande attualità ma che non è il caso di cantare vittoria e, al contrario, occorre rafforzare l'impegno per fornire ai cittadini strumenti informativi per difendersi da truffatori sempre più ingegnosi e preparati.



Scopri le nostre iniziative



www.adiconsum.it



progetti@adiconsum.it

Adiconsum, nell'ambito di Noi&UniCredit, realizza numerose iniziative dedicate all'educazione e alla promozione di comportamenti etici, sostenibili ed inclusivi rivolti a consumatrici e consumatori di ogni età. Dalla parità di genere alla finanza sostenibile, Adiconsum è sempre dalla tua parte!

