CONFCONSUMATORI
CONFEDERAZIONE GENERALE DEI CONSUMATORI
NOTIZIE

Agosto 2022
n.1

CHI HA PAURA DEL WEB?
LA RETE, TRA RISCHI E OPPORTUNITÀ

1

news

Speciale CHI HA PAURA DEL WEB?

Viviamo connessi. Ormai navigare su internet è una costante nella quotidianità di ognuno di noi: sul web inviamo messaggi, acquistiamo beni e servizi, progettiamo vacanze e gestiamo i nostri conti correnti. Purtroppo, però, insieme alle potenzialità, aumentano anche i rischi per chi naviga in rete. **"Chi ha paura del web?"**, a cui è dedicato questo numero di "Confconsumatori Notizie", è l'iniziativa di Confconsumatori nata con l'obiettivo di informare e formare i cittadini per metterli al sicuro dai rischi digitali e per aiutarli a sfruttare al meglio le opportunità che oggi internet offre.

Le **truffe digitali** sono sempre più sofisticate e diffuse, ed è importante conoscerne le diverse caratteristiche per sapere come tutelarsi. Phishing, spoofing, SIM swapping sono alcune delle tipologie più comuni. Hanno nomi diversi, ma l'obiettivo in genere è lo stesso: sottrarre i dati e le credenziali di accesso di carte e conti correnti, e rubare denaro alla persona malcapitata. All'interno di questo numero troverai la descrizione dei metodi di raggiro più utilizzati negli ultimi tempi, insieme ad alcuni consigli da mettere in pratica per cercare di scongiurare una truffa.

In ogni caso, non dobbiamo scoraggiarci e dobbiamo ricordare che, grazie alla presenza di alcuni servizi online – forniti, ad esempio, dagli Uffici della Pubblica Amministrazione, dal Servizio Sanitario Nazionale, o dalle Forze dell'Ordine – possiamo risparmiare tempo e risorse. Il web può rivelarsi un prezioso alleato e, se impariamo a conoscerlo, non dobbiamo averne paura!

Per restare aggiornato e scoprire tutte le attività previste all'interno dell'iniziativa "Chi ha paura del web?" ricorda di consultare l'indirizzo: www.confconsumatori.it/chi-ha-paura-del-web/.

in questo numero

Periodico di informazione ai consumatori
Direttore Responsabile: Antonio Bertoncini
Registro Stampa Tribunale di Parma, n. 3 del 14/03/2000
Questa testata usufruisce di contributi a sostegno dell'editoria speciale periodica a tutela dei consumatori e degli utenti ai sensi del d.lgs. 15 maggio 2017, n. 70.
Realizzazione grafica e stampa: Graphital Parma

Finanziato dal MiSE. Legge 388/2000 - ANNO 2021

TRUFFE BANCARIE ONLINE: QUALI SONO E COME FUNZIONANO

Molti nomi, un solo obiettivo: impossessarsi di dati e credenziali e accedere ai tuoi conti correnti. Ecco le truffe più comuni da cui devi stare in guardia:

PHISHING: si tratta di e-mail fraudolente che, all'apparenza, potrebbero assomigliare in tutto e per tutto a quelle inviate dalla tua Banca: di solito, infatti, riproducono – oltre al nome – i loghi e la grafica utilizzati nelle mail autentiche. Controlla bene ogni dettaglio e confrontale con le comunicazioni precedenti della tua Banca: potresti trovare piccoli errori o differenze, spie della truffa.

SIM SWAPPING: i truffatori sono in grado di prendere abusivamente il controllo della scheda SIM del tuo cellulare, dopo avere scoperto i tuoi dati magari inviandoti un virus. In questo modo, possono cercare di contattare la Banca a tuo nome e ottenere le tue credenziali di accesso all'home banking. Stai attento ai segnali: il tuo telefono potrebbe funzionare in modo anomalo o perdere il segnale!

SMS SPOOFING: potrebbe capitarti di ricevere, all'interno di conversazioni autentiche con Banche e intermediari finanziari, dei messaggi provenienti dai truffatori. Anche se il numero è lo stesso della Banca, è molto probabile che il messaggio contenga link sospetti che rimandano a siti esterni, magari "specchio" del sito reale della banca: prima di cliccare, telefona direttamente alla tua filiale per avere conferma della veridicità della comunicazione.

SPAMMING: specifichiamo che non sempre lo spamming coincide con una truffa. Si tratta in realtà di messaggi indesiderati inviati a un gran numero di utenti senza consenso, che spesso i gestori di posta elettronica filtrano in modo automatico (se così non accade, possiamo spostarli noi nella cartella "posta indesiderata" ed eventualmente bloccare il mittente). È bene fare attenzione però: in alcuni casi le comunicazioni indesiderate contengono link e allegati che nascondono virus, attraverso i quali i truffatori possono ottenere le nostre credenziali.

I CONSIGLI PER DIFENDERE I TUOI DATI

Ci sono casi in cui la truffa è così ben architettata da risultare praticamente inevitabile, ma molto spesso siamo noi i primi a non fare tutto il possibile per evitare di essere ingannati. In rete esistono numerose guide, a partire da quelle realizzate dagli stessi istituti bancari, che raccolgono consigli per proteggere i propri dati e, di conseguenza, i propri risparmi.

Ne è un esempio il vademecum realizzato da **ABI e Polizia di Stato**, in collaborazione con le associazioni dei consumatori. Come viene ricordato nella guida, "*le banche non chiedono mai, né tramite posta elettronica, né telefonicamente, né con messaggi sms, le credenziali di accesso al conto e i codici delle carte del cliente*". Inoltre, non inviano mai e-mail contenenti link se non nell'ambito di un processo avviato dall'utente (es. modifica e-mail personale, aggiornamento documento di riconoscimento...). Se riceviamo una comunicazione di questo tipo, dovremo subito avvertire la banca.

Un altro accorgimento che può sembrare scontato, ma che è imprescindibile per garantire la sicurezza dei nostri dati, è quello di avere sempre attivo sul proprio pc **un antivirus di qualità e aggiornato**. Soprattutto quando utilizziamo un pc che non è nostro, dobbiamo poi ricordare di chiudere la sessione effettuando il log-out. Infine, è sempre preferibile digitare personalmente l'indirizzo della propria banca e non cliccare su indirizzi già memorizzati nel pc.

Ricorda di custodire con cura le tue **credenziali**: mai conservare il PIN della carta di credito insieme alla stessa e mai divulgarlo a terzi, per nessun motivo. Se siamo imprudenti e vengono effettuate transazioni non autorizzate a nostre spese, difficilmente l'intermediario potrà rimborsarci.

Cerca poi di non essere prevedibile: quando crei una password, evita nome e data di nascita magari, per giunta, riciclandoli per siti diversi: i malviventi accederanno facilmente! Scegli una combinazione alfanumerica (ossia di lettere e numeri) - meglio ancora se non contenente parole comuni riconoscibili - e alterna caratteri maiuscoli, minuscoli e speciali.

Un'idea? Crea un **acronimo** da una frase per te significativa.
Esempio: "Mi chiamo Mario Rossi e abito a Parma!" sarà "McMReaaP!"
Maggiore è il tempo che viene impiegato per violare il nostro account, più aumenta la possibilità per noi di accorgerci se ci vengono notificati tentativi di accesso falliti.

I SERVIZI DELLA RETE

Se impari a fidarti della rete, scoprirai che ci sono molte pratiche che puoi sbrigare online, risparmiando tempo ed energie. Ecco alcuni riferimenti che potrebbero esserti utili:

FASCICOLO SANITARIO ELETTRONICO:

Il Fascicolo Sanitario Elettronico (www.fascicolosanitario.gov.it) è ormai attivo in tutte le regioni e ti permette di prenotare e pagare online prestazioni sanitarie, ma anche di consultare i tuoi referti. Consulta il tuo Fascicolo regionale per conoscere tutti i servizi offerti.

IL PORTALE DELL'AUTOMOBILISTA:

Questo portale del Ministero delle Infrastrutture (www.ilportaledellautomobilista.it) ti aiuterà in maniera rapida a verificare, ad esempio, il saldo punti della tua patente di guida o la classe ambientale di appartenenza (categoria Euro) di autoveicoli e motoveicoli. Potrai inoltre verificare la copertura assicurativa del tuo veicolo e consultare l'elenco delle officine autorizzate alla Revisione dei veicoli.

POLIZIA DI STATO:

Sul sito del Commissariato di Polizia di Stato online (www.commissariatodips.it) puoi inviare direttamente segnalazioni, denunciare reati telematici -come truffe digitali - o denunciare furti e smarrimenti.

CARABINIERI:

Anche il sito dei Carabinieri consente di presentare una denuncia di smarrimento o di furto ad opera di ignoti, attraverso l'indirizzo web: www.carabinieri.it/denuncia-via-web.

SEGNALA PREZZI:

Se hai notato dei cambiamenti anomali nei prezzi dei prodotti che acquisti solitamente, puoi inviare una segnalazione tramite il portale Segnala Prezzi del Ministero dello Sviluppo economico (https://segnalaprezzi.mise.gov.it/).

IL GARANTE DELLA PRIVACY

Il **Garante per la protezione dei dati personali**, anche chiamato Garante della Privacy (www.garanteprivacy.it), è l'autorità che si occupa, in sintesi, di verificare che i trattamenti dei dati personali siano conformi alla normativa in vigore. Il Garante ha poi il compito di formulare pareri e segnalare alle istituzioni competenti l'esigenza di intervenire con modifiche normative.
Sul sito del Garante – nella sezione **Modulistica e servizi online** - troverai alcuni strumenti destinati ai cittadini, come il modello per fare un reclamo con l'obiettivo di lamentare una violazione della disciplina in materia di protezione dei dati personali, oppure il modello per l'esercizio dei diritti in materia di protezione dei dati personali da indirizzare al titolare del trattamento dei dati personali di aziende, siti, pubblica amministrazione, banche, etc. Inoltre sono presenti modelli da compilare per segnalare episodi di cyberbullismo e per impedire pratiche di revenge porn su Facebook e Instagram.

CONTATTACI cerca le nostre sedi nell'area "Dove siamo" del sito **https://www.confconsumatori.it/gli-sportelli-di-confconsumatori/**

COME SOSTENERCI iscriviti o dona il 5xmille a **Confconsumatori 80025080344** per saperne di più **https://www.confconsumatori.it/sostienici/**

CONFCONSUMATORI