IN FAMIGLIA

PAGINE UTILI!

SMASCHERA LE TRUFFE DA COVID-19

Le insidie si sono moltiplicate

ALLA PORTA O VIA MAIL, AL TELEFONO O VIA SMS: **IMPARA A RICONOSCERE NUOVE E VECCHIE FORME DI RAGGIRO**

di Enrica Belloni

DJ LINUS, 63 ANNI
Si è fidato di un sms e gli hanno "fregato" 5 mila euro.

L'ultimo caduto nella rete è stato lo scrittore, giornalista e conduttore tv Corrado Augias: su *Repubblica*, nella risposta a una lettrice, ha commentato una mail in arrivo da Enel, lamentandosi per la forma sgrammaticata e sciatta. Ma il messaggio non era dell'azienda: era un tentativo (riuscito) di frode. Vale insomma la pena stare in guardia: **a ogni mail e a ogni sms, ma anche a ogni squillo di campanello**. In epoca Covid-19 si è infatti verificato un aumento delle truffe porta a porta, con motivazioni anche legate alla pandemia (vedi box nella pagina accanto).

DIETRO LO SCHERMO. Chi, dietro lo schermo di un pc, non avverte sensazioni di pericolo, sbaglia. Il fenomeno del *phishing* (vocabolo che associa il termine "*fishing*", pesca, con la sigla "ph", che rimanda alla pirateria informatica) «è cresciuto nei primi sei mesi del 2020 del 600% nel mondo», spiega Maria Rosaria Romano, dirigente del compartimento Polizia Postale della Campania: «La sola Polizia postale italiana ha trattato 98 mila situazioni». Le frodi più frequenti arrivano via mail: si riceve un messaggio che pare arrivare **dalla propria banca, dall'ente gestore della carta di credito o da una azienda**, per esempio Amazon o Enel, che chiede informazioni personali e dati di accesso a un servizio (password, nome e cognome, codice fiscale, numero della carta di credito...).
Poi ci sono gli sms truffaldini: simili a quelli della banca (il mittente è lo stesso), **chiedono di aggiornare i propri dati**. «Si parla in questo caso di "*smishing*", truffe via sms», aggiunge Romano. «Chi clicca ha accesso a un link che sembra vero ma è un clone dell'originale: da lì, se si inseriscono i dati, in pochi secondi i malviventi **possono sottrarre soldi o tenersi le informazioni per usarle poi**. Così, a volte, prima che la persona si accorga della frode, il denaro viene incassato o dirottato verso siti esteri».

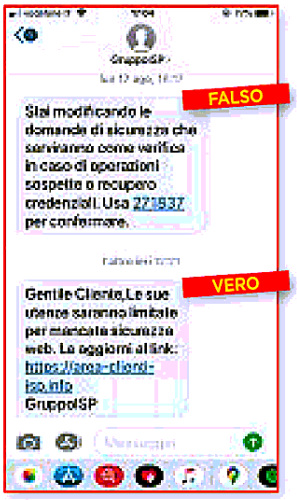
PUÒ CAPITARE A TUTTI. La prima cosa da fare se si è vittima di *phishing* o *smishing* è chiamare la propria banca o l'eventuale società di intermediazione. Prima si segnala, più semplice sarà prevenire o bloccare trasferimenti di denaro. «Poi, è bene **fare una denuncia alla Polizia postale**: si riacquista un po' di sicurezza e si aiutano le Forze dell'or-

VI CHIEDONO DATI SENSIBILI? ATTENZIONE
In genere le banche e le aziende non lo fanno via mail o sms.

> NON AGITE MAI D'IMPULSO MA LEGGETE SEMPRE BENE **E SOSPETTATE DI ERRORI E TONI CONFIDENZIALI**

 ● Nel 2020 il tema Covid è stato usato in oltre il 40% dei casi di *phishing* (Clusit, Associazione italiana sicurezza informatica)

CORRADO AUGIAS, 86
Ha messo i suoi dati rispondendo a una mail-truffa.



STESSO MITTENTE DELLA BANCA
Sopra, in alto, l'sms che invita a cambiare i propri dati è una truffa. Ma il mittente è lo stesso dell'istituto di credito: è difficile non venire raggirati. Subito sotto, un sms "vero" della banca.

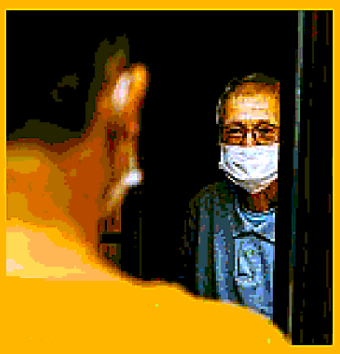
dine a sgominare le bande criminali. Trovate i numeri su *commissariatodips.it*. La denuncia può eventualmente essere raccolta anche a domicilio», aggiunge l'esperta. «**Non bisogna agitarsi, sentirsi in colpa o in imbarazzo**: può capitare a tutti, complici fretta o disattenzione, di cadere nel tranello».

DIFENDETEVI COSÌ. Per prevenire che ciò accada, dedicate la massima attenzione alle operazioni *on line* che coinvolgono soldi e dati sensibili e non agite mai d'impulso. **In genere, le banche o le aziende serie non richiedono dati via mail o sms**. Se avete un dubbio, fate una telefonata alla banca o al numero di assistenza clienti dell'ente da cui arriva il messaggio.
Leggete bene i messaggi: **errori ripetuti** sono un segno che deve mettere in allarme (com'è successo nel caso di Augias). Attenti ai caratteri: se sono strani, drizzate le antenne, fate lo stesso davanti a **indirizzi web molto lunghi** e che cominciano con "http://" e non "https://".
Spesso i testi sono anonimi e usano un **linguaggio improbabile, confidenziale** e In alcuni casi un po' intimidatorio.
Buona regola è **applicare un antispam** nella casella di posta del computer, che faccia da primo filtro delle false mail, e **cambiare spesso la password** adottando diversi criteri di scelta, usando punti, virgole e punti e virgola.
Quando siete in viaggio, prestate **attenzione alle reti wi-fi pubbliche**: sono comode e gratuite, ma connettendosi il rischio di subire attacchi da *hacker* è più alto, così come quello che qualcuno sottragga i dati.
Abituatevi a **trattare i codici di sicurezza** come il telefono o il computer: come una cosa preziosa, da conservare con attenzione.
Infine, attenti al "*vishing*", o *phishing* vocale: si riceve una telefonata, spesso da un sistema automatico, in cui si chiedono informazioni riservate, come avviene con le mail. Anche in questo caso, vale la regola che **non fidarsi è meglio**.

MARIA ROSARIA ROMANO
Dirigente compartimento Polizia postale della Campania.

Non fidatevi anche se sanno tutto di voi

C'è chi ti suona alla porta o al citofono, esibisce tesserini e divise della Croce rossa, della Protezione civile, o **dichiara di essere dipendente dell'azienda sanitaria che ha il compito eseguire un il tampone gratuito per il Covid-19** o di sanificare la casa, compresi soldi e gioielli. O ancora, c'è chi chiama fingendosi un parente alle prese con un problema, la malattia («nonna, ho preso il Covid»), o un incidente, e chiede soldi. È accaduto a Treviso, a Milano, a Trento. In realtà si tratta di truffatori che, una volta entrati in casa, estorcono o rubano denaro e oggetti preziosi. «**Succede sempre più spesso, soprattutto agli anziani, che in questo periodo sono più soli e vulnerabili**, perché hanno meno possibilità di avere vicino i famigliari», dice Roberto Messina, presidente di Senior Italia FederAnziani.
Per prevenire truffe e furti, **non aprite se non conoscete la persona, anche se chi ha suonato sa il vostro nome**, finge di essere amico dei vostri parenti, esibisce improbabili tesserini. Nessun ente manda personale a casa vostra per riscuotere o controllare soldi, neppure la Polizia. **Non date corda a chi al telefono si dichiara nipote, fratello, amico**. Nel dubbio, mettete giù con una scusa e richiamate il vero parente. Non tenete in casa grosse somme di denaro, gioielli e altri oggetti di valore. Se vi chiamano al telefono fingendosi un vostro parente e tentano di truffarvi, segnalatelo alle Forze dell'ordine. Se vi sentite in pericolo, **comunicatelo ai vicini**, alle famiglie del condominio, al custode. È importante non isolarsi. E se vi hanno truffato, non vergognatevi, è successo a tanti, ma **fate subito denuncia** a Polizia o Carabinieri.



FINGONO DI VOLERVI AIUTARE
I ladri possono offrirsi anche di farvi un tampone gratis.

● Il Comune di Milano ha stipulato la polizza AssicuraMi: rimborsa gli over 70 vittime di truffe