Testata: altroconsumo.it
Data: 5 ottobre 2021

Phishing: i consigli per difendersi

Segui - Tariffe internet, telefonia fissa e mobile

Il phishing è un sistema illegale che abili truffatori usano per raccogliere dati strettamente personali e usarli poi per scopi illeciti. Per non abboccare, occorre prestare attenzione ai siti che si visitano e alla posta che si riceve e imparare a distinguere il vero dal falso.

05 ottobre 2021

Email, ma anche sms, messaggi privati nei social network e nelle app di messaggistica: sono questi alcuni dei mezzi che i truffatori usano per prenderti all'amo e sottrarre dati anagrafici e codici di accesso a conti correnti e carte di credito. Una truffa digitale, che però può costare soldi veri.

Come funziona il phishing

Il metodo principale che i criminali utilizzano per arrivare ai tuoi preziosi dati è l'invio di **email**. Molto curate nell'aspetto, sembrano proprio provenire dalla banca o da un'altra fonte considerata attendibile. In genere contengono testi allarmanti che informano di problemi con il conto o con l'account, invitando a cliccare su un link dove poi ti sarà richiesto di inserire username, password, quando non direttamente i tuoi dati bancari. Il link in questione rimanda solo apparentemente al sito web del servizio a cui si è registrati. In realtà, porta a tutt'altro sito, per quanto nell'aspetto possa sembrare identico all'originale, gestito dai truffatori. Fornire i dati richiesti equivale a dare in mano a ladri di professione le **chiavi di accesso** per rubare i tuoi risparmi. Cadere nel tranello è più facile di quanto si possa pensare. E non succede solo ai più anziani. Siamo talmente abituati a ricevere email da banche, istituti di credito e altre simili realtà che può capitare di non prestare troppa attenzione al mittente e a come è confezionata l'email. E cliccare su un link è questione di un attimo. È quindi importante avere gli strumenti utili a **prevenire e contrastare** questo fenomeno e per aiutare i nostri figli o i nostri nonni a stare in guardia e comportarsi nel modo giusto.

Come comportarsi per non correre rischi

Il modo migliore per difendersi dal phishing è quello di **cancellare** immediatamente il messaggio sospetto senza mai rispondere, cliccare su link o scaricare programmi allegati. Ma come si fa a riconoscere un messaggio di phishing da uno vero? Ecco i **trucchi** per smascherare i tentativi di truffa e vivere il web in tranquillità.

- **Utilizza il buon senso** Se un messaggio chiede informazioni personali, può darsi che sia un modo per raccogliere indizi su di te e indovinare le tue password. Tieni poi a mente che le banche non mandano mai messaggi email o via chat in cui chiedono dati confidenziali. Lo stesso vale per proposte allettanti di ogni genere: se è troppo bella per essere vera, probabilmente è falsa.
- **Datti il tempo di riflettere prima di cliccare** E nel dubbio, non farlo. Esistono tecniche per far sì che una email sembri inviata da un indirizzo diverso da quello reale (per esempio, sembra che il mittente sia la tua banca ma in realtà è tutt'altro). È anche possibile inserire nel messaggio un link del tipo www.sitoufficiale.it, che in realtà porta da un'altra parte. Se usi il pc te ne puoi accorgere portando il mouse sul link (attenzione a non cliccare): nella parte in basso a sinistra della finestra vedrai l'indirizzo a cui realmente manda quel link.

- **Attiva gli avvisi sul cellulare** Le banche ti consentono di attivare un sistema di avvisi automatici: ogni volta che viene effettuato un addebito sulla tua carta, ti arriverà un messaggio sul cellulare. In questo modo puoi riconoscere subito un utilizzo fraudolento e bloccare tempestivamente la carta. È utile anche controllare regolarmente i propri estratti conto.
- **Stai attento agli sconosciuti** Se ricevi messaggi da mittenti sconosciuti o servizi che non hai attivato, non indirizzati esplicitamente a te o il cui contenuto è privo di senso, si tratta di spam. Non cliccare sui link presenti in queste email, nemmeno per curiosità. E non partecipare alle catene di Sant'Antonio. Entrambi i sistemi sono usati per confermare l'esistenza di indirizzi email (tra i milioni costruiti a caso dai phisher). Se abbocchi riceverai sempre più messaggi.
- **Digita l'indirizzo correttamente** Esistono numerosi siti con nomi molto simili a quelli di siti famosi o istituzionali (per esempio: facebok.com - con una O sola - o ancagenerali.it, senza la B iniziale). Siccome possono anche essere veicolo di phishing, la cosa migliore è digitare una volta l'indirizzo della tua banca, facendo attenzione a scriverlo correttamente, e poi salvarlo tra i preferiti del browser per il futuro.
- **Controlla gli indirizzi internet** La parte dell'indirizzo che identifica il proprietario del sito è quella subito prima del .com (ma anche .it, . org e così via). Per esempio: www.intesasanpaolo.com è un sito di proprietà di Intesa Sanpaolo, mentre www.intesasanpaolo.abc123.com appartiene al proprietario del sito abc123, che potrebbe non avere nulla a che fare con il gruppo bancario. Tieni presente, poi, che se un sito inizia con https:// preceduto da un lucchetto è un sito sicuro.
- **Tieni aggiornato l'antivirus** I sistemi più sofisticati non puntano al raggiro dell'utente, ma si basano sull'introduzione di virus da contrastare con contromisure informatiche (anti-malware).
- **Crea password sicure** Non sempre un phisher attacca direttamente la tua banca. A volte agisce in maniera più indiretta: anche un messaggio di semplice spam su Facebook può essere il primo gradino di un attacco. Proteggi tutti gli account con password adeguate.

Scarica il libro Interland: avventure digitali, che Google ha pubblicato in collaborazione con Altroconsumo, Polizia di Stato e Fondazione Mondo Digitale. Leggilo insieme a tutta la famiglia per scoprire come navigare sereni tra le infinite risorse del web

Contenuto realizzato in collaborazione con Google nell'ambito del progetto Vivi internet, al meglio