LA GUIDA

di **Antonio Scuglia**

Un agente della polizia postale al lavoro (immagine d'archivio)

«Truffe digitali, ecco come fanno a rubare i nostri dati e i nostri soldi»

Alberto Foggia, avvocato pisano dell'associazione consumatori Adusbef, spiega le nuove tecniche dei "pirati" e cosa possiamo fare per respingerli

Pisa La tentata truffa della falsa email con il "ricatto a luci rosse" segnalata dal *Tirreno* nei giorni scorsi è solo la punta dell'iceberg. «Il mondo digitale – spiega l'avvocato Alberto Foggia, legale Adusbef di Pisa, – offre innumerevoli vantaggi ma nasconde anche molte insidie. Le truffe online sono sempre più sofisticate e diffuse, mettendo a rischio i nostri dati personali e finanziari. Nella giungla di truffe digitali quelle più diffuse sono: phishing, smishing, vishing spoofing, spear phishing, caller id, catfishing, man in the browser e business email compromise».

Ma in cosa consistono? Come cercare di non diventarne vittima e come tutelarsi una volta truffati? Alberto Foggia tratta molto frequentemente questi casi, ricevendo richieste di tutela dai cittadini della nostra provincia e non solo. Fare il punto della situazione con i casi che cura più frequentemente può essere utile anche per capire quali sono le "nuove frontiere" di questi pericoli, e soprattutto come difendersi e – nello sfortunato caso in cui si sia cascati nell'inganno – come rimediare nei limiti del possibile.

Avvocato Foggia, andiamo con ordine. Cosa sono phishing, smishing e vishing?

«Il primo è la truffa più comune. Gli artefici inviano email o messaggi apparentemente provenienti da Istituti bancari, aziende o servizi online conosciuti, chiedendo di cliccare su link o allegati "maligni" per così sottrarre le nostre credenziali di accesso. Lo smishing è simile al phishing, ma avviene tramite Sms. Si riceve un messaggio che invita a cliccare su un link per verificare un'operazione bancaria, aggiornare un servizio o vincere un premio. Il vishing sfrutta il telefono per ingannare le vittime. I truffatori, impersonando spesso istituzioni finanziarie, aziende note o enti governativi, contattano le loro potenziali vittime tramite chiamate o messaggi vocali. L'obiettivo è quello di carpire informazioni sensibili come numeri di carte di credito, codici di accesso online, dati personali o altre credenziali che possono essere utilizzate per compiere azioni fraudolente».

Si parla molto anche dello spoofing.

«Il truffatore si finge un altro soggetto, come un amico, un parente, un dipendente di un'azienda o personale di una Banca, per ottenere informazioni sensibili».

E lo spear phishing?

«Una variante più mirata del phishing in cui l'hacker dispone già di informazioni sulla vittima (può ad esempio conoscere i suoi dati personali, come la carta d'identità ed il numero di conto carpiti tramite il cosiddetto "dark web", ovvero dei siti web nascosti, cui si può accedere solo con particolari software, ove oltre a trovare dati sensibili di persone, sono praticate anche altre attività illegali quali spaccio di droga, vendita armi, pedopornografia) e personalizza l'"attacco" per renderlo più credibile».

Ci parla del Caller Id?

«Il truffatore può sfruttare la tecnologia del Caller ID, mostrando sul display del telefono un numero apparentemente affidabile (come quello della Banca in cui il destinatario della telefonata ha il conto o, ad esempio ultimamente, della Polizia o dei Carabinieri) per indurre la vittima a rispondere e fornire informazioni sensibili. Ciò avviene grazie ad applicazioni reperibili sul web».

L'avvocato Alberto Foggia, legale per Pisa e provincia dell'Adusbef, associazione a difesa dei consumatori e degli utenti

> Bisogna sempre stare attenti e non condividere informazioni personali

> Anche se siamo cascati nel tranello, spesso c'è modo di evitare il danno con una denuncia

Più diffuso sui social è il catfishing...

«Che consiste nel creare un falso profilo online per ingannare le persone e instaurare relazioni sentimentali o amicizie con lo scopo di ottenere denaro o altre forme di vantaggio».

E insidiosissimo è il "man in the browser".

«Un tipo di "attacco" che permette al truffatore di intercettare e modificare le informazioni che vengono inserite nel browser, come le password o i dati della carta di credito».

Cos'è il business email compromise?

«I truffatori hackerano le caselle di posta elettronica e modificano l'Iban all'interno di fatture o pro forma già ricevute. Il nome del beneficiario rimane invariato, ma l'Iban viene sostituito con uno errato che dirotta il pagamento verso il truffatore».

Queste sono le armi dei truffatori. Ma come possiamo difenderci?

Sicuramente diffidare dalle richieste sospette: non cliccare su link o allegati contenuti in email o messaggi, soprattutto se provengono da mittenti sconosciuti o comunque con acronimi improbabili. Poi, verificare l'identità del mittente: assicurarsi sempre che l'indirizzo email o il numero di telefono indicato sia autentico, contattando subito l'apparente mittente per conferma. Inoltre, utilizzare password "forti" e diversificate: creare "password complesse" per ogni account online e attivare l'autenticazione a due fattori; esistono siti internet ove vengono create "password complesse" (ovvero una combinazione di caratteri che rende difficoltoso all'hacker decifrarle) nonché conservate tutte insieme tipo "cassaforte". E tenere aggiornato il software: installare sempre gli ultimi aggiornamenti di sicurezza per il proprio sistema operativo ed i programmi (cosiddetto antivirus) . Fare attenzione ai social network: non condividere informazioni personali in modo indiscriminato e diffidare dalle richieste di amicizia da parte di sconosciuti. Infine, controllare l'Iban del destinatario del bonifico: prestare la massima attenzione in occasione dei pagamenti, soprattutto a seguito del ricevimento di una fattura con un Iban diverso da quello consueto e, quindi, riscontrarlo prima col beneficiario».

E come tutelarsi una volta subita la truffa?

Non appena resosi conto della truffa perpetrata ai suoi danni, l'interessato, se si tratta di truffa bancaria, deve disconoscere l'operazione contestata tramite appositi moduli presso l'Istituto di Credito o anche con propria comunicazione e chiederne allo stesso il rimborso. In ogni caso, presentare denuncia presso la polizia giudiziaria (carabinieri o polizia o guardia di finanza) . Trascorsi 15 giorni dal disconoscimento-reclamo, in caso di diniego al rimborso o di mancato riscontro, l'utente potrà presentare ricorso all'Arbitro bancario finanziario (Abf) se si tratta di questione che vede coinvolto un istituto di credito o similare».

Il ricorso all'ABF è vantaggioso?

«Sì, tanto per una questione tempistica (l'intera procedura fino alla decisione richiede circa 8-10 mesi) e di rischi, visto che non comporta, in caso di mancato accoglimento del ricorso, alcuna condanna nei confronti di controparte a spese legali di sorta. Il ricorso può essere proposto anche direttamente dall'interessato, ma l'ausilio di un professionista è preferibile visto il particolare tecnicismo della materia».

Il libro

Phishing e nuovi attacchi informatici: le strategie difensive

A proposito di truffe digitali, segnaliamo la pubblicazione in materia della collana giuridica che l'avvocato Foggia cura con il collega Edoardo Ferragina, ovvero "Phishing e nuovi attacchi informatici. Modalità operative e strategie difensive" scritta dall'Avv. Francesco Cocchi, che si può acquistare su Amazon (https://www.amazon.it/Phishing-informatici-operative-strategie-difensive/dp/8894863069).

Adusbef, associazione a difesa dei consumatori e degli utenti, particolarmente specializzata nel settore bancario nacque nel maggio 1987. Ha sempre combattuto battaglie in difesa dei diritti dei cittadini in ogni settore consumerista con gli esclusivi contributi degli iscritti, rifiutando contributi privati che possono condizionare anche indirettamente l'attività, spiega la stessa associazione. L'Adusbef ha circa 175 sedi in Italia ed è membro della Federazione Utenti Bancari Europei fondata con associazioni di Spagna, Francia, Olanda, Gran Bretagna.

«L'Associazione – si legge nello Statuto – opera sul territorio nazionale e locale per informare, promuovere, assistere, tutelare, rappresentare e difendere i diritti e gli interessi individuali e collettivi dei cittadini, dei consumatori e degli utenti in genere». Ha come scopo esclusivo «la tutela dei diritti e degli interessi dei cittadini, dei consumatori e degli utenti». L'Adusbef pisana può essere contattata presso l'avvocato Alberto Foggia: tel. 050.542786, fax 050.7911566, email foggiamerico@gmail.com