FURTO D'IDENTITÀ

I delinquenti propongono affari online non chiedendo alcuna somma in denaro, ma solo la conferma di alcuni dati. Ovviamente, tra tali dati ci sono anche quelli bancari o le informazioni sensibili (tra cui le password) utili ad aprire linee di credito presso le banche del soggetto truffato o direttamente per rubare soldi. I furti di identità sono quelli che costringono le vittime a passare più tempo nel tentativo di riparare a tutti i danni fatti dai ladri.

COME FUNZIONA

Gli autori dei furti di identità ottengono informazioni personali, tra cui password, numeri di documenti di identità e numeri di carte di credito o di sicurezza sociale utilizzandoli per scopi illeciti e agire in modo fraudolento a nome del malcapitato. Questi dati sensibili potrebbero essere utilizzati per scopi illeciti, ad esempio richieste di mutuo, acquisti online o accesso a informazioni mediche o finanziarie della vittima.

Il furto di identità è strettamente legato al phishing e ad altre tecniche di ingegneria sociale che vengono spesso utilizzate per carpire informazioni sensibili dalla vittima. Anche i profili sui social network o di altri servizi online noti possono essere utilizzati come fonte di dati, contribuendo ad aiutare i criminali a spacciarsi per le vittime.

Una volta raccolte queste informazioni, gli autori dei furti di identità possono utilizzarle per ordinare merci, aprire conti correnti e/o mutui, impossessarsi degli account online delle vittime o, più in generale, intraprendere azioni legali a loro nome.

Recentemente, sono avvenuti anche casi di false proposte di lavoro tramite siti internet, nelle quali veniva richiesta copia dei documenti e selfie del candidato, utilizzando poi questi dati e foto per l'apertura di rapporti bancari.

In seguito a queste attività illecite, le vittime potrebbero subire perdite finanziarie dovute a prelievi ed acquisti non autorizzati effettuati a loro nome. O, peggio ancora, potrebbero essere ritenuti colpevoli delle azioni compiute dai malfattori ed essere oggetto di indagini condotte dalle forze dell'ordine, oppure essere tenuti al pagamento di spese legali, avere uno status di merito creditizio modificato a loro insaputa e subire così anche un danno reputazionale.

FURTO D'IDENTITÀ

COME DIFENDERSI

Proteggi la tua connessione: se hai intenzione di utilizzare le tue informazioni online, assicurati di farlo utilizzando una connessione sicura, preferibilmente una rete domestica o aziendale o una rete dati cellulare. Se possibile, evita Wi-Fi pubbliche non protette da password.

Proteggi i tuoi dispositivi da software dannosi e autori di attacchi utilizzando una soluzione di protezione affidabile ed aggiornata.

Diffida da messaggi e siti sospetti: non trasmettere foto, selfie, copia di documenti a soggetti di cui non vi è certezza di serietà; effettua accertamenti prima di inviare quanto richiesto.

Cura la qualità delle password: crea password efficaci lunghe, difficili da indovinare e univoche (preferibilmente contenenti caratteri maiuscoli, minuscoli, numeri e caratteri speciali).
Non utilizzare mai la stessa password per più di un account o servizio. In questo modo, anche se gli autori di un attacco riescono a indovinare la password, il danno sarà limitato solo all'account (o al servizio) compromesso.

Presta particolare attenzione ai dati sensibili: se desideri eliminare documenti fisici contenenti informazioni personali, assicurati di farlo in modo sicuro rendendoli irrecuperabili o distruggendoli. Lo stesso vale per i dispositivi elettronici: Se decidi di vendere o smaltire vecchi smartphone, tablet o laptop, assicurati di cancellare tutti i dati sensibili contenuti.

Evita di condividere troppi contenuti: in un'era in cui la maggior parte degli utenti possiede più di un account sui social network, la condivisione eccessiva di contenuti potrebbe rappresentare un grosso problema. Specialmente se post, foto o video contengono informazioni sensibili che potrebbero essere utilizzate in modo illecito per rubare la tua identità. Evita di postare questi contenuti e di fornire molti dettagli sulla tua vita o storia personale che potrebbero essere utilizzati da malintenzionati per agire a tuo nome.