Truffe bancarie, phishing e loro conseguenze

Progetto “Digitalmentis 2”

Iniziativa Competenze Digitali finanziata dal Fondo MIMIT per i consumatori - D.M. 31/07/2024

TRUFFE ONLINE

Il termine indica un **reato che viene commesso, appunto, online tramite siti web e applicazioni** per smartphone. In generale, è molto più facile per i criminali informatici truffare chi naviga in rete piuttosto che tentare di farlo tramite interazioni faccia a faccia.

Metodologie di truffe:

PHISHING

Il termine **“phishing”** è una **variante di “fishing”** (letteralmente **"pescare" in lingua inglese**), allude all'uso di tecniche sempre più sofisticate per **"pescare" dati finanziari e password di un utente.** Sono truffe appunto che cercano di ottenere informazioni personali, come password o numeri di carta di credito, fingendo di essere entità affidabili.

Si tratta di un’attività illegale che sfrutta una **tecnica di ingegneria sociale**, il malintenzionato effettua un **invio massivo di messaggi** che **imitano, nell’aspetto e nel contenuto, messaggi legittimi di fornitori di servizi**; tali messaggi fraudolenti **richiedono di fornire informazioni riservate** come, ad esempio, il **numero della carta di credito o la password** per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali **messaggi sms** o **chiamate**.

Metodologie di truffe:

VISHING: (termine derivante dalla combinazione di **Voice** - contatto vocale - e **Phishing**) è una tipologia di frode telefonica in cui **i malintenzionati telefonano all'ignara vittima** (fingendosi, ad esempio, operatori della Banca **sostenendo di fornire assistenza tecnica, ma in realtà cercando di ottenere accesso ai dati**) **inducendola a fornire informazioni personali**, finanziarie o di sicurezza, quali i codici segreti della banca o delle carte.

SMISHING: come il Vishing, ma usando **sms** invece di chiamate (**sm**ishing = **sms**). I malintenzionati **si intromettono nelle conversazioni sms già in essere tra clienti e istituti bancari/poste/**ecc... e, **fingendosi i mittenti legittimi, inducono le vittime a fornire informazioni personali e/o cliccare su fraudolenti link forniti**.

Tecnica dello SPOOFING

Consiste nel **“mascherare”/falsificare** l'**identità di un mittente** (ad esempio, un **indirizzo email**, un **numero di telefono** o un **indirizzo internet**) **per ingannare un utente** o un sistema. L'obiettivo è **impersonare un'entità fidata**, **come** una **banca o** un **servizio clienti**, **per indurre la vittima a compiere azioni dannose**, come cliccare su link, scaricare malware o fornire dati sensibili.

Metodologie di truffe:

CLONE PHISHING: è un tipo di phishing in cui una mail **legittima viene modificata negli allegati o nei link** e rimandata ai riceventi, dichiarando di essere una versione aggiornata. **Le parti modificate della mail sono volte a ingannare il ricevente**. Questo attacco sfrutta la fiducia che si ha nel riconoscere una mail precedentemente ricevuta.

CLONAZIONE DELLA SIM TELEFONICA (SIM Swap): il fenomeno consiste nella **duplicazione fraudolenta della SIM telefonica** del cliente da parte di criminali, **al fine di impossessarsi del numero di cellulare del cliente**. In questo modo **il frodatore**, una volta entrato in possesso del numero di telefono del cliente, **si sostituisce a lui con la possibilità**, ad esempio, di **autenticare e confermare operazioni effettuate fraudolentemente c**on il profilo del cliente, oppure **intercettare gli SMS sia in ingresso che in uscita dal numero telefonico del cliente.**

Segnali di avvertimento di una truffa online:

- **Richieste di pagamento immediato o pressione psicologica**, tramite e-mail e telefonate;

- **URL** (Uniform Resource Locator) ovvero **nomi di indirizzi di siti sospetti o e-mail che** sembrano non autentiche e **chiedono di cliccare su qualche link** che porta a siti non di nostra conoscenza (prima è bene informarsi su che sito stiamo inconsapevolmente navigando);

- **Grammatica o ortografia scadenti** nei messaggi.

Suggerimenti per proteggersi dalle truffe online:

- Mantenere il **software e** gli **antivirus aggiornati**;
- Utilizzo di metodi di **autenticazione a due fattori**;
- Essere **cauti con i messaggi sospetti ed e-mail** poco chiare;
- Utilizzare **password sicure e diverse per ogni account**;
- Fare **attenzione a** offerte troppo allettanti o **richieste di pagamento immediate**;
- **Utilizzare una VPN**(virtual private network = rete privata virtuale), ovvero un **servizio online che nasconde la tua attività online e la tua posizione reale**. Questo processo maschera il tuo indirizzo IP e crittografa i dati di navigazione, rendendoli inaccessibili a chiunque altro.

Le VPN sono consigliate soprattutto quando si utilizza una rete Wi-Fi pubblica.

Grazie

Progetto “Digitalmentis 2”

Iniziativa Competenze Digitali finanziata dal Fondo MIMIT per i consumatori - D.M. 31/07/2024