PHISHING

Cos'è?

Il phishing è un **tipo di truffa** effettuata via **internet, sms** o **telefono**. I malintenzionati la utilizzano per ottenere **informazioni riservate**, fingendosi qualcuno o qualcosa di cui la vittima si **fida**.

Non sottovalutare il phishing

Presta sempre **attenzione**: la distrazione è il vettore di errore più comune: causa il **98%** delle violazioni mentre l' **86%** avviene tramite l'uso di **credenziali rubate**. (fonte).
Le e-mail di **phishing** sono in **continuo aumento**. Gli autori di phishing sono veloci nell'**adattare la comunicazione** agli argomenti di maggiore interesse - guadagni, rimborsi fiscali, annunci sulla salute o proposte di lavoro, etc - e nell'adottare **nuove tecniche comunicative** per indurre a condividere file apparentemente innocui.

Quali sono le informazioni riservate?

Sono informazioni che permettono di **ricostruire** un **profilo esaustivo** per procedere al **furto di identità**. Password e nome utente sono un esempio di informazioni riservate e a rischio phishing, perché consentono l'uso malevolo della casella di posta, dell'area riservata o di altri servizi.

Come funziona?

Il malintenzionato contatta la vittima con una richiesta **e-mail ingannevole**, spesso ottimamente costruita per renderla il più possibile **verosimile e coerente** con il **finto mittente.** Il tono della comunicazione può risultare **minaccioso e/o urgente**.

Solo via email?

NO, la richiesta delle informazioni può avvenire anche attraverso una **telefonata** di un finto operatore, un **SMS**, una **pagina web clonata**, un **canale social.**

Difendersi, si può?

SI, buon senso, **prudenza** e un **po' di diffidenza**: i codici personali, le password, i dati bancari e altri dati riservati **non sono mai richiesti** nei modi su indicati. Alla pagina: https://www.unipg.it/sicurezza-on-line/riconosci-e-proteggiti-dal-phishing, trovi le indicazioni aggiornate per difenderti dai rischi del phishing.