Veris s.r.l.
Medical Systems

Informativa Phishing

Il phishing è una truffa online in cui criminali informatici si fingono entità attendibili (banche, siti famosi, istituzioni) tramite email, SMS o chiamate per rubare dati sensibili come password e numeri di carte di credito.

È una forma di ingegneria sociale che crea urgenza per indurre le vittime ad agire, spesso cliccando su link fraudolenti.

Necessita porre molta attenzione in quanto questi messaggi, attraverso le nuove tecnologie sembrano sempre più veritieri.

Sia Noto che la società VERIS S.r.l. non chiederà mai

Password, PIN o dati della carta di credito

via email o SMS.

Informativa Phishing

Esempi di Phishing:

- **Email di falsi avvisi bancari**: Messaggi che segnalano un'attività sospetta sull'account e richiedono di accedere tramite un link per verificarlo, portando a una falsa pagina web.
- **Virus informatici**. Le modalità di infezione sono diverse. La più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf . Nel caso si tratti di un c.d. “financial malware” o di un “trojan banking”, il virus si attiverà per carpire dati finanziari. Altri tipi di virus si attivano allorquando sulla tastiera vengono inseriti “user id e password”, c.d. “keylogging”, in questo caso i criminali sono in possesso delle chiavi di accesso ai vostri account di posta elettronica o di e-commerce.
- **Smishing (SMS Phishing):** SMS che annunciano un premio, un pacco bloccato o un blocco della carta, chiedendo di inserire dati personali su un sito fasullo.
- **Vishing (Phishing Vocale):** Telefonate da un finto operatore bancario che cerca di ottenere codici OTP o credenziali per sbloccare il conto.
- **Clone Phishing**: E-mail che replica un messaggio legittimo già inviato, sostituendo link o allegati con versioni dannose.

Informativa Phishing

Sinonimi e Termini Correlati:

Truffa online / Frode informatica

Ingegneria sociale (la tecnica psicologica alla base)

Smishing (SMS phishing)

Vishing (Voice phishing)

Spear phishing (attacco mirato a una persona specifica)

Caratteristiche Principali:

Urgenza: Il messaggio spesso ha carattere di urgenza e richiede di cliccare, aggiornare o verificare il conto immediatamente a pena del blocco del conto bancario o della carta di credito.

Esche: L'uso di nomi di marche note e loghi contraffatti per creare fiducia.

Informativa Phishing

Cosa fare in caso di messaggio sospetto:

- Non cliccare mai sui link contenuti nel messaggio.
- Digitare manualmente l'indirizzo del sito ufficiale nel browser.
- Controllare il Mittente e Verificare che l'indirizzo email o il numero di telefono sia quello ufficiale.
- Verificare la correttezza grammaticale del messaggio.
- Verificare la congruità dei loghi presenti sul messaggio con quelli originali
- Verificare la presenza delle firme e della frase di trattamento dati facenti riferimento al regolamento della privacy

Procedere alla comunicazione scrivendo all'indirizzo amministrazione@veris.it dettagliando:

- La ricezione del messaggio anomalo spiegandone il contenuto (non inoltrare il messaggio).
- L'indirizzo da dove proviene il messaggio.
- La richiesta di effettuare le opportune verifiche su messaggi dubbi.

Informativa Phishing

VERIS S.R.L.

VIA CAMPORELLE N. 11, 10020 CAMBIANO (TO)

C.F. e P.I. 07285990011

TEL. (+39) 0119442.83 - FAX (+39) 0119438961

E-mail: info@veris.it PEC: info@pec.veris.it

Web: www.veris.it

Certificazioni: ISO9001 - ISO14001- ISO45001 - ISO13485 - UNI/PDR125 - ISO27001

Le Policy Aziendali si possono visualizzare sul nostro sito web