Nicolosi, 15 aprile 2023

Al personale
Agli alunni
Alle famiglie

Oggetto: Social Engineering e truffe telefoniche

Social Engineering

Anche se hanno molti punti in comune, phishing e social engineering non sono affatto la stessa cosa. In alcuni casi, il social engineering è "propedeutico" al phishing, soprattutto in caso di attacchi mirati verso un numero limitato di vittime.
Detto anche **ingegneria sociale**, il social engineering è una tecnica che fa forza su leve psicologiche e comportamentali per ottenere dalla vittima dati sensibili e personali. L'obiettivo finale è lo stesso del phishing, anche se le strade che vengono percorse per ottenere quei dati sono più variegate.
A differenza delle altre tipologie, l'ingegneria sociale non sfrutta alcuna falla o vulnerabilità software ma sfrutta delle "vulnerabilità" psicologiche degli utenti, andando a giocare sulle loro abitudini online. Terminata la fase di "studio", il cybercriminale passa a quella di attacco: sfruttando i social o le piattaforme di messaggistica avvicina l'utente, provando a entrare in confidenza con lui tanto da confidargli dati e informazioni che potrebbero tornargli utili.

Truffe telefoniche

Capita sempre più spesso che i possessori di smartphone siano vittime di truffe telefoniche di ogni genere, che puntano a rubare soldi (sia dal conto telefonico, sia dal conto corrente) o dati utili a impadronirsi dell'identità dell'intestatario della SIM.
Per riuscirci, i cybertruffatori utilizzano tecniche che variano a seconda dell'obiettivo da raggiungere. In alcuni casi possono essere più aggressivi e diretti; in altri utilizzano degli schemi che puntano prima di tutto ad acquistare la fiducia dell'utente, per poi colpirlo "nell'intimità".
Analizziamo le truffe più comuni:

1 - Sim swap

Data anche la sua "giovane età", è considerata essere una delle più pericolose, soprattutto per i rischi che comporta sul fronte della protezione dell'identità personale.

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it

SIM Swap sta, letteralmente, per "scambio di SIM" e comporta il "furto" del proprio numero di telefono.
Diffuso soprattutto negli Stati Uniti, viene utilizzato per accedere ai profili personali protetti da verifica in due passaggi. Questa tecnica prevede che il criminale conosca la reale identità della vittima, ovviamente il numero di telefono e altri dati personali. Una volta che ha raccolto queste informazioni, il truffatore si presenta in un negozio oppure chiama il servizio clienti del provider dei servizi di telefonia e usa le informazioni personali raccolte per convincere il commesso/l'operatore a **disabilitare la SIM legittima e "spostare" il numero di telefono del truffato su una nuova SIM in suo possesso.** A questo punto potrà utilizzarlo per accedere alla casella di posta elettronica, profilo social o, ancora peggio, al conto corrente bancario facendosi inviare i codici di accesso ai profili via SMS.

2 - Smishing
Si tratta dell'equivalente telefonico del phishing. Solo che, al posto dei messaggi di posta elettronica, vengono utilizzati gli SMS. Nonostante cambi il "mezzo di trasmissione", le modalità di attacco e gli obiettivi dei cybertruffatori sono gli stessi: furto di credenziali, di informazioni personali o di denaro.

3 - Vishing
Deriva dalle parole inglesi "Voice" e "Phishing", il vishing viene detta anche **truffa del consenso rubato.** Il cybertruffatore crea un sistema di chiamate automatizzato che consente di contattare un numero elevato di persone in pochissimo tempo.
Il vishing può essere declinato in vario modo: dalle chiamate dei call center che riescono a "estorcere" il nostro consenso per un cambio di operatore o fornitore di servizio alle truffe ben più articolate, grazie alle quali impossessarsi dei dati personali dell'utente.

4 - Wangrid
Detta anche "truffa dello squilletto", si palesa tramite chiamate brevissime o singoli squilli provenienti da numeri di telefono esteri- La speranza dei truffatori è che l'utente provi a richiamare il numero: al primo squillo verranno addebitate cifre elevatissime (anche diversi euro per pochi secondi di chiamata) o attivati abbonamenti settimanali indesiderati e difficilissimi da disdire.

Il Responsabile della Sicurezza Informatica
Ing. Prof. Salvatore Musumeci
Salvatore
Musumeci
15.04.2023
14:46:13
GMT+01:00

Il Dirigente
Luciano Maria sambataro
LUCIANO MARIA
SAMBATARO
16.04.2023 12:03:13
GMT+01:00

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it