Lezione 21 del 17/04/2025

Truffe

Corso android per smartphone

Docenti Dott.ssa Roberta Lai Ing. Massimo Terrosu

cadadie.it

Truffe: tipologie su smartphone

Le 3 tipologie più comuni di attacco

1 Phishing

Phishing via e-mail

2 Smishing

Phishing via SMS

3 Vishing

Phishing via telefono

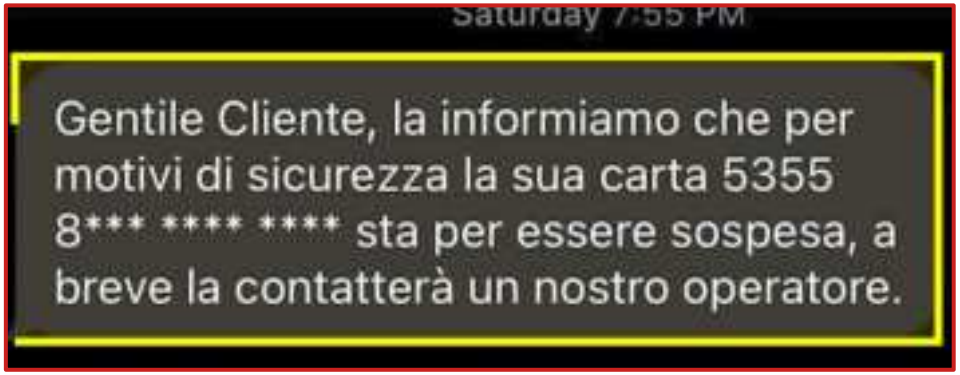
COSA LE CARATTERIZZA (Ingegneria Sociale)

- ✓ Richiesta di un'azione da compiere con urgenza
- ✓ Richiesta di informazioni sensibili
- ✓ Presenza di link o allegati da scaricare

- ✓ Offerta imperdibile o intervento di sblocco
- ✓ Urgenza per non perdere l'occasione o per intervenire
- ✓ Presenza di un link che indirizza a un sito malevolo

- ✓ Chiamata dalla banca o organizzazione conosciuta
- ✓ Senso di urgenza legato a un possibile rischio
- ✓ Richiesta di informazioni sensibili, pin, numeri carte

Phishing via telefono o chiamata telefonica (vishing)



«Abbiamo ricevuto il tuo curriculum»: come funziona la nuova (e diffusissima) truffa telefonica in Italia

L'interlocutore si finge un'azienda o un'agenzia per il lavoro e promette un impiego allo scopo di estorcere dati personali sensibili. Alle volte, secondo diverse testimonianze, viene mandato un link che dovrebbe rimandare a moduli da compilare per il datore di lavoro, e in altri casi invece l'interlocutore invita a fare investimenti in sospette piattaforme online, promettendo guadagni veloci.

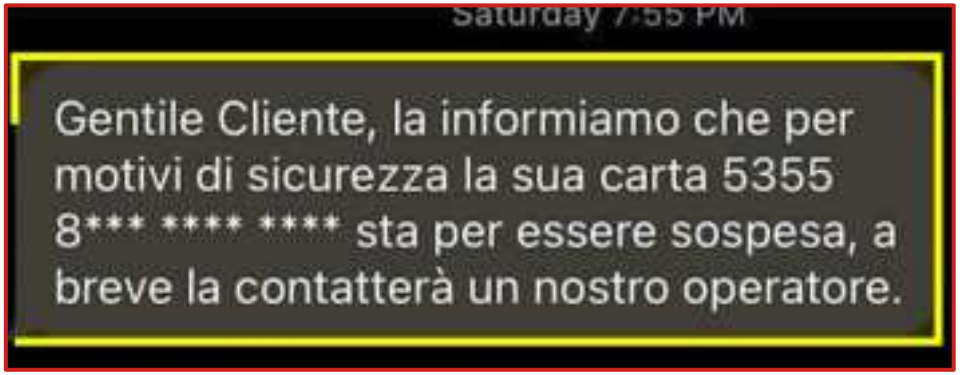
Truffa del doppio SPID: come proteggersi

- **Consapevolezza e Vigilanza.**
- **Autenticazione a Due Fattori (2FA.)**
- **Verifica Periodica degli IBAN.** Registrarsi su portali pubblici per rilevare eventuali variazioni.
- **Gestione cauta dei Dati e delle comunicazioni.** Accedere sempre ai siti ufficiali digitando l'indirizzo direttamente nel browser.
- **Monitoraggio degli Account e Password Sicure.** Utilizzare password complesse e uniche per ogni servizio.
- **Segnalazione di Attività Sospette legate al furto di identità.** Rivolgersi alla Polizia Postale e all'AgID (Agenzia per l'Italia Digitale).
- **Monitoraggio del Conto Corrente.** Nei mesi successivi a un presunto furto di dati attivando gli alert bancari
- **Verificare periodicamente gli SPID attivi a proprio nome.** Controllare sul sito dell'Agenzia per l'Italia Digitale (AgID) quali identità digitali risultano attive a proprio nome e segnalare eventuali anomalie. La segnalazione all'AgID può contribuire al blocco del secondo SPID fraudolento.

Truffa del doppio SPID: cosa fare se si è vittima della truffa

- **Sporgere immediatamente denuncia alla Polizia Postale.** Tramite il commissariato di Polizia Postale online
- **Avvisare tempestivamente l'Identity Provider (gestore dell'identità digitale) che ha rilasciato le credenziali SPEED.** Cambiare subito la password di SPID per impedire a chi ha commesso la truffa di continuare a utilizzarla.
- **Bloccare immediatamente le carte coinvolte e contattare la propria banca.**
- **Monitorare attentamente i movimenti del proprio conto corrente anche nei mesi successivi.**
- **Altroconsumo fornisce una lettera di reclamo per richiedere il rimborso alla banca.**
- **Agire rapidamente.**

Phishing via telefono o chiamata telefonica (vishing)



«Abbiamo ricevuto il tuo curriculum»: come funziona la nuova (e diffusissima) truffa telefonica in Italia

L'interlocutore si finge un'azienda o un'agenzia per il lavoro e promette un impiego allo scopo di estorcere dati personali sensibili. Alle volte, secondo diverse testimonianze, viene mandato un link che dovrebbe rimandare a moduli da compilare per il datore di lavoro, e in altri casi invece l'interlocutore invita a fare investimenti in sospette piattaforme online, promettendo guadagni veloci.

Phishing via telefono o chiamata telefonica (vishing)

- **Mezzo di attacco**: Chiamate automatizzate o da operatori che si fingono banche o enti governativi.
- **Pericolosità**: Alta, particolarmente convincente per la componente umana.
- **Diffusione**: Alta, specialmente verso anziani e persone vulnerabili.
- **Difesa**: Non fornire mai dati personali o bancari a chiamate in entrata, richiamare l'ente utilizzando il numero ufficiale, utilizzare app di filtraggio chiamate.

Truffa dello squillo riagganci dopo un solo squillo e di solito più volte al giorno.L'obiettivo è quello che l'utente richiami così da addebitargli gli alti costi di una telefonata all'estero.

Truffa del Robocall rispondendo al telefono, si viene accolti da un messaggio registrato che ti porta ad azioni improprie.

Truffa del SÌ: l'obiettivo è quello di far rispondere con un "sì" a domande di qualunque tipo. L'obiettivo è quello di autorizzare addebiti o contratti tramite estrapolazione del "si" dal contesto.

Phishing via telefono o chiamata telefonica (vishing)

- **+375** (Bielorussia)
- **+371** (Lettonia)
- **+381** (Serbia)
- **+255** (Tanzania)
- **+216** (Tunisia)
- **+44** (Regno Unito)
- **+373** (Moldavia)
- **+383** (Kosovo)
- **+ 53** (Cuba).

Tariffe a tempo

Al chiamante verrà addebitato il costo della chiamata in base ai minuti di conversazione, le tariffe quindi dipendono dai minuti effettivi di conversazione.

	IL TUO GUADAGNO		COSTO PER IL CHIAMANTE	
	AL MIN	SCATTO	AL MIN	SCATTO
Profilo T7	0,09	-	0,38	0,168
Profilo 01	0,129	-	0,54	0,168
Profilo 02	0,17	-	0,68	0,17
Profilo 03	0,26	-	0,77	0,127
Profilo 04	0,342	-	0,99	0,127
Profilo 07	0,418	-	1,23	0,138
Profilo 08	0,38	0,06	1,68	0,759
Profilo 09	0,451	-	1,29	0,118
Profilo 10	0,64	0,01	1,88	0,217
Profilo 11	0,64	0,013	1,88	0,217
Profilo 12	0,518	-	1,489	0,006
Profilo 13	0,65	-	1,91	0,309
Profilo 14	0,738	0,06	2,10	0,516
Profilo 15	0,51	0,06	1,57	0,738
Profilo 16	0,751	0,056	2,28	0,53

Phishing tramite codice QR (quishing)

- **Mezzo di attacco**: Codici QR manipolati che portano a siti fraudolenti.
- **Pericolosità**: Media, dipende dal sito di destinazione.
- **Diffusione**: In rapida crescita negli ultimi anni con l'aumento dell'uso dei QR code.
- **Difesa**: Utilizzare app di scansione QR che mostrano l'URL prima di aprirlo, verificare l'URL di destinazione, essere cauti con QR code in luoghi pubblici.

Truffa del QR code (Quick Response) può contenere stringhe alfanumeriche

QR per pagamenti online tramite app bancarie (poche verifiche)

QR come URL (contengono link a siti web di phishing)

QR come numero di telefono fake

Google lens
aprire Google Lens e inquadrare il codice QR

App sistema
Camera>Impostazioni>Esegui scansioni codici QR

Dal menù di scelta rapida>Scansione codice QR

Truffa del doppio SPID: come funziona

Clonazione Identità

Raccolta dati sensibili (CI, TS, selfie, su social /web tramite phishing e/o dark web)

Attivazione Secondo SPID

All’insaputa dell'utente. Le PA permettono due SPID con stesso CF ma diverso numero telefono e Mail

Accesso ai Portali

Entrata nei sistemi governativi (INPS, Agenzia delle Entrate, Sistema Sanitario

Modifica Dati

In particolare l’IBAN

Dirottamento Fondi

Pensione, rimborsi 730, firma digitale documenti, attivazione abbonamenti, apertura conti correnti….

Truffa del doppio SPID: come proteggersi

- **Consapevolezza e Vigilanza.**
- **Autenticazione a Due Fattori (2FA.)**
- **Verifica Periodica degli IBAN.** Registrarsi su portali pubblici per rilevare eventuali variazioni.
- **Gestione cauta dei Dati e delle comunicazioni.** Accedere sempre ai siti ufficiali digitando l'indirizzo direttamente nel browser.
- **Monitoraggio degli Account e Password Sicure.** Utilizzare password complesse e uniche per ogni servizio.
- **Segnalazione di Attività Sospette legate al furto di identità.** Rivolgersi alla Polizia Postale e all'AgID (Agenzia per l'Italia Digitale).
- **Monitoraggio del Conto Corrente.** Nei mesi successivi a un presunto furto di dati attivando gli alert bancari
- **Verificare periodicamente gli SPID attivi a proprio nome.** Controllare sul sito dell'Agenzia per l'Italia Digitale (AgID) quali identità digitali risultano attive a proprio nome e segnalare eventuali anomalie. La segnalazione all'AgID può contribuire al blocco del secondo SPID fraudolento.

Truffa del doppio SPID: cosa fare se si è vittima della truffa

- **Sporgere immediatamente denuncia alla Polizia Postale.** Tramite il commissariato di Polizia Postale online
- **Avvisare tempestivamente l'Identity Provider (gestore dell'identità digitale) che ha rilasciato le credenziali SPEED.** Cambiare subito la password di SPID per impedire a chi ha commesso la truffa di continuare a utilizzarla.
- **Bloccare immediatamente le carte coinvolte e contattare la propria banca.**
- **Monitorare attentamente i movimenti del proprio conto corrente anche nei mesi successivi.**
- **Altroconsumo fornisce una lettera di reclamo per richiedere il rimborso alla banca.**
- **Agire rapidamente.**