White Paper

Come evitare le truffe via SMS e WhatsApp

L'ARTE DELLA TRAPPOLA 2.0

Se c'è una categoria di persone che finora non ha avuto bisogno di particolari incentivi per modernizzare la propria attività adottando tempestivamente e in maniera creativa gli strumenti informatici e di comunicazione più moderni è indubbiamente quella dei delinquenti.

Sotto l'elegante etichetta della **cybercriminalità** si nasconde un mondo assai variegato per obiettivi, capacità tecniche e canali d'azione che è tuttavia accomunato da una grande capacità di sfruttare le nuove opportunità man mano fornite dal progresso tecnologico per ampliare le proprie attività illegali.

Ormai abbiamo già imparato a convivere con malware, virus e attacchi informatici di ogni sorta, tutelandoci in genere con un minimo di accortezza e, soprattutto, con il ricorso ad applicazioni e servizi gestiti che ci assicurano una protezione in linea con le nostre esigenze - siano esse personali, di una piccola attività piuttosto che di una grande azienda.

Ma, come ruggine che non dorme mai, i tecnodelinquenti del XXI secolo **non smettono un istante di cercare nuove strade per raggiungere i loro obiettivi** e nuovi anelli deboli in una catena che si allunga di giorno in giorno schiudendo possibilità inedite per colpire vittime inconsapevoli.

Fai finta per un attimo di entrare nella testa di uno di questi personaggi.

Sai che c'è un'intera industria specializzata nella protezione informatica che erige muri sempre più solidi per impedirti di accedere a reti e sistemi. La ricerca di nuove vulnerabilità è ormai questione iper-tecnica appannaggio di squadre di esperti organizzate quasi come vere aziende. Il **Dark Web offre, spesso a cifre ragionevoli, strumenti e servizi di ogni tipo**: ma anche questi sono costantemente tenuti d'occhio e facilmente neutralizzati prima di che tu possa rientrare dell'investimento.

Dove andare a colpire, allora?

UNA MINACCIA CHE VIENE DA LONTANO

Per decenni e fino almeno alla metà degli anni Novanta **sono circolate in tutto il mondo curiose missive nelle quali perfetti sconosciuti si rivolgevano a destinatari scelti a caso** dagli elenchi telefonici (te li ricordi?) **proponendo una qualche fantasiosa transazione finanziaria** riguardante lo spostamento di grosse somme di denaro da qualche remota nazione esotica a fronte di grasse provvigioni.

È la famigerata "truffa nigeriana", così chiamata perché sviluppatasi proprio in Nigeria dove tuttora alimenta un'industria illegale fiorente.

Le lettere erano scritte da qualcuno che si spacciava per un principe o un alto funzionario governativo di quel Paese africano. Chi cadeva nella trappola, ingolosito dalle cifre promesse, si trovava ben presto sommerso dalle richieste di **sborsare "anticipi" per presunte imposte o "mance"** necessarie a sbloccare i fondi promessi. Da piccole somme si saliva ben presto a importi di rilievo, andando avanti più a lungo possibile fintanto che la vittima non si rendeva conto - alla buon'ora - della truffa in cui era caduta.

Ti sembra impossibile che qualcuno possa dare credito a una storia del genere, vero?

Eppure questa bella pensata ha avuto talmente tanto successo da guadagnarsi un intero articolo del codice penale nigeriano che punisce questo genere di frode (o "scam" in inglese): si tratta dell'articolo 419, motivo pe il quale è spesso conosciuta anche come "419 scam".

E poiché le idee che funzionano trovano facilmente nuovi adepti**, la truffa è ben presto uscita dai confini nigeriani diffondendosi praticamente ovunque** nel mondo con numerose variazioni sul tema: vedove di dittatori con la necessità di spostare soldi di nascosto, direttori di banca alle prese con conti dormienti da liquidare, persino responsabili di enti di beneficenza bisognosi di aiuto per incassare donazioni milionarie: la fantasia regna sovrana.

Un sistema del genere, tanto efficace, **non poteva rimanere vincolato a lungo a un mezzo di comunicazione lento, poco affidabile e relativamente oneroso come la corrispondenza postale**.

La diffusione di Internet e della posta elettronica è stata, in questo senso, **una manna dal cielo**: basta un click per raggiungere milioni di destinatari a costi irrisori, promuovendo una vera e propria industria del crimine che sa mungere come pochi altri quello zerovirgola di creduloni che continuano a credere a queste storie farlocche. D'altra parte, come direbbero gli esperti di marketing, è sufficiente un tasso di redemption dello 0,001% su una campagna di 10 milioni di invii per acquisire ben 100 clienti - o, in questo caso, vittime.

L'evoluzione della truffa nigeriana costituisce un caso da manuale per rendersi conto di come i malintenzionati siano rapidi nel percepire i vantaggi che la nuova tecnologia può offrire per facilitare le loro attività illecite. A maggior ragione quando si pensi che gli scammer nigeriani sono passati alla posta elettronica ai tempi in cui molte aziende nostrane viaggiavano ancora col fax, e questo nonostante l'infrastruttura per la comunicazione dati nell'Africa occidentale fosse all'epoca poco diffusa, poco affidabile e molto costosa.

Da allora sono trascorsi anni e il settore tecnologico ha messo in campo le proprie contromisure sotto forma di **filtri antispam sempre più sofisticati** che, agendo a livello di server se non addirittura su un livello infrastrutturale più alto, fanno piazza pulita di buona parte di questo genere di messaggi senza che tu te ne accorga nemmeno. E anche quando una mail sospetta riesce a passare attraverso le maglie della protezione, certamente hai imparato a guardarla con occhio molto critico e riconoscerla per quello che è.

Missione compiuta e problema risolto, allora? Certamente no, perché **nel frattempo i cybertruffatori non sono rimasti a loro volta con le mani in mano e hanno presto identificato un nuovo, promettente campo d'azione** legato alla tecnologia che ha ridefinito il nostro modo di vivere quotidiano negli ultimi quindici anni: **gli smartphone e la comunicazione mobile**.

DOVE SONO TUTTI?

Basterebbe considerare il solo punto di vista numerico per capire come gli smartphone siano un canale irrinunciabile per cercare di contattare il più grande numero possibile di vittime potenziali. A novembre 2020 circolavano nel mondo 3,5 miliardi di smartphone e 4,8 miliardi di telefonini, il che si traduce rispettivamente nel 45% e nel 60% circa dell'intera umanità.[1] Non male, considerando che gli utenti della posta elettronica sono 3,9 miliardi[2] ma con qualche differenza importante:

- La prima: come detto, **sulla posta elettronica sono stati sviluppati nel tempo una serie di strumenti di difesa automatizzata** che rendono difficoltoso il passaggio delle mail truffa. La comunicazione che transita su smartphone e telefonini, da questo punto di vista, è invece ancora del tutto scoperta.
- Seconda differenza: **le persone sono sempre più abituate a considerare con sospetto i messaggi di posta elettronica** che arrivano da destinatari sconosciuti o con contenuti inaspettati. C'è invece **meno attenzione nei confronti dei messaggi che arrivano tramite telefono**, generalmente perché di solito vengono inviati da mittenti conosciuti.

Il primo punto è strettamente legato al fatto **che i sistemi di comunicazione in uso nella telefonia mobile sono del tutto proprietari e "chiusi"**.

Gli SMS arrivano direttamente dal tuo operatore, non da un tuo server aziendale che puoi attrezzare con software antivirus o antispam, né tanto meno da un servizio gestito per il filtraggio e la protezione della posta come quelli a cui si affidano sempre più imprese. Di fatto, ti becchi gli SMS così come ti vengono mandati, senza alcun controllo sui contenuti né sulla reputazione del mittente.

Vogliamo parlare di WhatsApp?

Anche qui, il sistema è completamente chiuso e l'unica "protezione" prevista è la semplice segnalazione che viene fatta quando un messaggio arriva da un numero di telefono che non è presente nella tua rubrica dei contatti (solo dopo aver ricevuto un primo messaggio da uno sconosciuto ti sarà possibile bloccarlo). **I messaggi possono contenere di tutto**, anche link che ti mandano su siti infestati di malware, perché WhatsApp non effettua alcun controllo salvo bloccare i profili che vengono segnalati come fastidiosi, indesiderati o spammer da un numero sufficiente di utenti... ovviamente *solo dopo* che questi abbiano ricevuto ed evidenziato messaggi sospetti.

Vedi bene come nel mondo della comunicazione mobile gli operatori abbiano pensato a tante cose fuorché alla sicurezza. Non è una loro priorità ed è bene tenerlo sempre a mente. Qualcuno ha proposto, scherzosamente ma non troppo, di incollare sugli smartphone un adesivo con la dicitura: "ATTENZIONE! Dispositivo vulnerabile! Truffatori in agguato!". Sarebbe un modo low-tech ma efficace per ricordarsi di essere cauti ogni volta che lo si utilizza.

L'intero concetto di comunicazione mobile è dunque vulnerabile o comunque privo di tutte quelle protezioni tecniche che circondano la posta elettronica. Ma poi c'è un secondo elemento che rende davvero goloso questo canale per i truffatori, e riguarda il fattore umano.

1 https://www.bankmycell.com/blog/how-many-phones-are-in-the-world
2 https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide

Rifletti un attimo sul rapporto che hai con il tuo smartphone e su ciò che esso rappresenta per te:

- È un dispositivo che ti accompagna lungo tutta la giornata nel lavoro, nel tempo libero e nei rapporti sociali.
- È uno strumento che ti permette non solo di comunicare ma, sempre più spesso, di provare la tua identità, di fare acquisti, di consumare servizi e contenuti.
- È associato a un numero di telefono che non si trova su elenchi pubblici (sempre che tu ne faccia un uso accorto) e che fornisci solamente ai tuoi contatti.
- È il tuo modo per restare in collegamento col mondo ricevendo e inviando informazioni in modo istantaneo.

Se mettiamo insieme tutto questo, otteniamo un oggetto che:

a) tocca continuamente tutte le sfere della tua vita privata e pubblica;

b) **sei abituato a utilizzare con fiducia**;

c) **invita a essere usato in tempo reale abituandoti a reazioni quasi d'impulso**.

Una miscela davvero pericolosa perché, di fatto, la sua familiarità lo fa entrare all'interno di quel delicato perimetro entro il quale una persona si muove generalmente con soglie di attenzione più basse del solito.

I cybertruffatori lo sanno benissimo e da tempo hanno messo a punto strategie efficaci, pur se a volte elementari (ma la semplicità è un'arma a loro favore, in questo senso), per colpire le potenziali vittime su un terreno a essi favorevole.

Vediamo come funziona il meccanismo per capirci meglio.

Tutto inizia quando **ricevi un messaggio da un mittente che si spaccia per qualcuno che conosci** o di cui ti fidi.

A volte è un'organizzazione con cui probabilmente hai a che fare, come una banca, un ente pubblico, un operatore di telecomunicazione, una catena di negozi e via dicendo. **Altre volte invece si tratta di un amico, un conoscente o un collega**: sono i casi più subdoli, in genere frutto di una precedente violazione del PC, dello smartphone o del profilo online di uno dei tuoi contatti, di cui viene utilizzata la rubrica proprio per dare credibilità al contenuto inviato.

Contenuto che può essere di vario genere: è qui, infatti, che la creatività dei truffatori ha briglia sciolta avendo l'obiettivo di farti compiere un'azione (in genere fare click su un link) distraendoti a sufficienza per evitare che tu possa prestare troppa attenzione - e quindi magari iniziare a sospettare - a quanto ti viene chiesto di fare.

Il codice spedito "per sbaglio".

Una delle truffe più in voga e delle più pericolose, dal momento che il suo obiettivo è quello di rubarti completamente l'account di un certo servizio. Il suo funzionamento è abbastanza semplice, e per capire come funziona prendiamo l'esempio di un malintenzionato che voglia sottrarti il tuo account WhatsApp.

Se ti è mai capitato di dover cambiare numero telefonico, sostituire il telefono o riconfigurare il tuo smartphone da zero avrai notato come **WhatsApp controlla che tu sia effettivamente il proprietario del numero di telefono** che indichi per accedere al servizio inviandoti un "codice di controllo" via SMS.

Una volta che digiti quel codice all'interno della app WhatsApp, il servizio ha la certezza che tu sia effettivamente in possesso del numero di telefono che usi per accedervi. È un sistema pratico e semplice che viene usato da moltissimi altri servizi, quindi presta attenzione perché adesso arriva il bello.

Immagina un cybertruffatore che conosca il tuo numero di telefono: dal *suo* smartphone potrà installare WhatsApp e tentare di configurarlo specificando il *tuo* numero. WhatsApp riceverà la richiesta e, come abbiamo visto, invierà un SMS di verifica al *tuo* cellulare.

Qui scatta la trappola: **il malintenzionato ti contatta in modo pressoché contestuale** facendo finta di essere per esempio l'assistenza clienti di WhatsApp piuttosto che un tuo contatto conosciuto (le modalità variano ma la sostanza rimane) **chiedendoti di girargli il contenuto dell'SMS di verifica** che hai appena ricevuto in modo inaspettato.

La scusa suona in genere come: "Ti abbiamo mandato un codice per sbaglio, puoi rimandarcelo?" oppure "Stiamo verificando la sicurezza del tuo account, comunicaci il codice che abbiamo inviato al tuo numero".

Nel momento in cui tu dovessi rispondere fornendo il codice richiesto, **il truffatore potrà convalidare il proprio tentativo di accesso a WhatsApp** sottraendoti di fatto l'account e iniziando a impersonarti acquisendo man mano l'accesso anche ad altri servizi come la posta elettronica, i drive virtuali in cloud, i servizi finanziari e di pagamento... Puoi solo immaginare come questo possa essere solamente l'inizio di un vero e proprio incubo per te, dal momento che il furto di identità è uno dei crimini più dannosi e complessi da neutralizzare per chi ne cade vittima.

WhatsApp Gold, il silenzio è d'oro.

Restiamo sempre nell'ambito di WhatsApp con un altro schema che si ripete a ondate cicliche. La pretesa è che **WhatsApp sta per cambiare la propria politica commerciale e tornare ad essere un servizio a pagamento**, come nei primi anni di funzionamento precedentemente alla sua acquisizione da parte di Facebook.

Ma dal momento che sei un affezionato utente di WhatsApp, ecco che ti viene offerta l'esclusiva possibilità - fortunello che sei - di installare la versione Gold (o Premium) della relativa app che ti consentirà di continuare a usare il servizio gratuitamente. Segue link all'app store per poter scaricare l'applicazione.

Ovviamente WhatsApp non ha cambiato il proprio modello commerciale - non è più a pagamento da molti anni perché i ricavi provengono dall'utilizzo dei dati personali, di traffico e di contatto per sostenere l'intera filiera dei servizi del gruppo Facebook, Instagram compreso - e **la presunta app Gold o Premium non è altro che un perfetto esempio di malware ospitato su un app store parallelo**, non ufficiale, che spalanca le porte del tuo smartphone a pubblicità indesiderate, virus, sottrazione di dati e tutto il resto dell'arsenale dei cybercriminali.

Esiste un'altra e più semplicistica versione di questa truffa legata al presunto WhatsApp a pagamento, che invita semplicemente l'utente a saldare con carta di credito l'abbonamento annuale al servizio. L'importo è in genere poca cosa proprio per non destare troppi sospetti; l'importante per chi sta dietro a questi meccanismi è poter raccogliere i dati personali e delle carte di credito delle vittime. Le informazioni così acquisite potranno essere sfruttate per acquisti illeciti e/o vendute a pacchetti nei marketplace specializzati che pullulano all'interno del Dark Web.

Il segreto della segreteria.

Non sono più in auge come un tempo, ma **le segreterie telefoniche esistono ancor**a - naturalmente in versione digitale - e qualcuno continua a usarle. La notifica di un messaggio che aspetta di essere ascoltato nella nostra casella di segreteria telefonica desta certamente curiosità; dovrebbe invece destare molta cautela ogni volta che proviene da un servizio che in realtà non contempla una funzione del genere.

È la truffa della segreteria di WhatsApp, che ovviamente non esiste (quantomeno non esiste attualmente), veicolata attraverso messaggini che mettono in bella evidenza un pulsante attraverso il quale poter ascoltare una presunta registrazione a noi destinata.

Il pulsante non conduce a nessuna segreteria e nessuna registrazione, ma attiva un programma che di solito rastrella i contenuti dello smartphone sottraendo dati personali, foto, video e tutto quello che può riguardare la vita personale della malcapitata vittima.

Carissimo sconto.

È tempo di promozioni. Saldi stagionali, Black Friday, Cyber Monday, svuotamento magazzini a scopo di inventario, rinnovamento dell'assortimento, pronti per la scuola, svendite dovute alla crisi, feste stagionali, varie ed eventuali. In ogni momento dell'anno il settore del retail trova sempre un buon motivo per lanciare offerte speciali ai consumatori - in modo del tutto lecito, intendiamoci.

Ma **queste occasioni vengono cavalcate facilmente anche da chi propone falsi buoni sconto** per acquisti presso famosi nomi dell'e-commerce o note catene della grande distribuzione come supermercati e ipermercati, negozi di elettronica e così via.

Come non approfittare di questo imperdibile colpo di fortuna? Il coupon per lo sconto (in alternativa il premio vinto in qualche fantomatico concorso o sondaggio) va però attivato online sul sito del "negoziante": allo scopo **viene fornito un link che punta a un sito dal nome simile a quello ufficiale, simile in ogni suo aspetto all'originale ma che, dietro la facciata di ufficialità, nasconde il truffatore di turno** che non attende altro - come minimo - di poter carpire i tuoi dati personali che tu stesso gli fornirai, convinto di fare un affare.

CAMBIANO LE STORIE MA LO SCHEMA È SEMPRE LO STESSO

Come vedi, le storie che vengono costruite dietro i messaggi truffaldini possono essere molto diverse tra loro.

Oggi circolano soprattutto quelle che abbiamo appena visto, nelle quali il protagonista è spesso WhatsApp. Domani ne verranno inviate di altre, vuoi perché dopo un po' di tempo le persone si fanno più consapevoli, vuoi perché ci saranno altri servizi che saliranno sulla cresta dell'onda con le loro vulnerabilità e le loro caratteristiche pronte da sfruttare ex novo per tentare di acchiappare nuove vittime.

Non sappiamo oggi quali narrative verranno usate per creare nuove storie come quelle viste finora, ma possiamo scommettere che tutte saranno accomunate da alcuni punti fermi che è bene tenere a mente per evitare di cascarci:

- ***Un senso di urgenza***. Il truffatore non vuole che tu ti fermi a ragionare sul messaggio che hai ricevuto: il suo scopo è di spingerti ad agire subito, prima che ti possa fare qualche domanda e renderti conto del reale obiettivo della comunicazione che ti è appena arrivata.

- ***Un senso di familiarità***. Il messaggio mostra di provenire quasi sempre da contatti affidabili (per esempio quelli che si trovano nella tua rubrica telefonica o tra i tuoi contatti WhatsApp) o comunque credibili (un brand noto con cui è facile che tu abbia a che fare).
- ***Un senso di necessità di agire***. Il contenuto del messaggio ti offrirà sempre un presunto vantaggio, come un buono sconto, un abbonamento a prezzo promozionale, la vincita di un premio o una app per continuare a usare gratis un certo servizio. In alternativa a carote del genere possono essere usati anche dei bastoni sul tono di "conferma il tuo account altrimenti lo chiudiamo" oppure "ci risulta che tu abbia commesso un reato informatico, contattaci per spiegazioni".

Per questo il telefonino è un mezzo assai apprezzato da questa categoria di cybercriminali: come abbiamo visto prima, **il fatto che tu sia abituato a usarlo d'impulso e che generalmente venga utilizzato per contattarti da persone che conosci ha la conseguenza psicologica di farti trovare più facilmente distratto o con le difese abbassate**.

Né la tecnologia può aiutarti più di quel tanto, poiché come detto ci troviamo in un territorio privo di quegli strumenti di protezione automatica che da tempo hai imparato ad apprezzare e utilizzare sui tuoi PC di casa e dell'ufficio.

Cadere in trappola con WhatsApp, SMS e applicazioni per la comunicazione su smartphone è davvero semplice, ma il problema non finisce qui. **Se ti venisse la malsana idea di condividere qualche messaggio truffaldino con i tuoi contatti, magari spinto dal messaggio stesso ("un'offerta imperdibile solo per te e per i tuoi amici!"), non faresti altro che avviare una catena di illeciti trasformandoti in complice dei malintenzionati**. Qualcuno dei tuoi conoscenti potrebbe chiederti conto del tentativo di coinvolgerlo nella truffa, e nel caso migliore faresti una ben magra figura intaccando la tua reputazione.

Ora, quando si parla di questo genere di truffe via smartphone, la reazione delle persone è spesso la stessa: "Ma il mio numero di telefono lo conoscono solo poche persone fidate". Un approccio del genere è ancora più dannoso perché implica nell'utente un grado di fiducia ancora maggiore nei messaggi che riceve.

Conoscere il numero di telefono di una certa persona può essere più o meno difficile, ma il punto è che queste attività vengono solitamente svolte in modo automatizzato tentando combinazioni di numeri a tappeto.

Peggio ancora quando vieni contattato perché un malintenzionato è riuscito in precedenza a violare il profilo un tuo conoscente che ha il tuo numero in rubrica: in questo caso la richiesta arriverebbe direttamente da un nominativo fidato (o meglio, dal suo account), aumentando le probabilità che tu risponda senza farci particolare caso.

Il consiglio è allora quello di **applicare sempre un po' di sano senso critico ogni volta che vieni contattato da chiunque** - anche se teoricamente una persona conosciuta - qualunque sia il canale usato per raggiungerti. **Non fidarti mai delle apparenze** e prima di rispondere cerca di capire se il messaggio sia legittimo o meno, verificando col preteso mittente (ma utilizzando un canale di comunicazione diverso, nel caso quello usato sia stato compromesso) o anche ricercando sul web la presenza di eventuali allerta o aggiornamenti sulle truffe online del momento. A volte può essere utile anche confrontarsi con qualcuno di cui ti fidi, resteresti sorpreso della facilità con cui ci si può rendere conto dell'inconsistenza di certi messaggi solamente provando a spiegarne i contenuti a qualcun altro.

E se proprio non riesci a evitare istintivamente quella pericolosa accoppiata "fiducia + impulso" che contraddistingue il normale utilizzo degli smartphone, potrai sempre prendere in considerazione la possibilità di attaccarci un adesivo che ti ricordi di fare attenzione.

Glossario

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

Malware – Combinazione dei termini inglesi "malicious" (malevolo, pericoloso, illecito) e "software". Indica l'insieme degli strumenti software che i cybercriminali utilizzano per entrare nei computer delle loro vittime, assumerne il controllo in modo parziale o integrale, propagarsi all'interno della rete colpita ed effettuare attività illecite come la sottrazione di dati personali o sensibili, lo spionaggio, l'invio di messaggi di posta indesiderata o il blocco crittografico dei dati a scopo di riscatto. Ognuna di queste attività assume una propria denominazione, come spyware, spamware, ransomware ecc.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, concettualmente simili ma accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

SMS Short Message Service – Servizio che permette l'invio di brevi messaggi di testo da 160 caratteri di lunghezza attraverso la rete telefonica. Reso possibile dalla definizione degli standard GSM del 1985, il servizio SMS ha dovuto attendere sette anni prima di essere implementato effettivamente, raggiungendo in breve un successo su scala planetaria che prosegue ancora oggi nonostante la concorrenza dei servizi di messaging basati su Internet come WhatsApp, Telegram, Viber, iMessage e Facebook Messenger.