Phishing 2.0, ecco le truffe digitali che ingannano anche gli esperti

Il phishing 2.0 combina ingegneria sociale e tecnologie avanzate per colpire con maggiore efficacia. Email, chiamate vocali e messaggi WhatsApp diventano strumenti di frode difficili da riconoscere anche per utenti esperti (Fonte: https://www.agendadigitale.eu/ 1°ottobre 2025)

Il phishing 2.0 rappresenta l'evoluzione più sofisticata delle truffe digitali, capace di sfruttare tecniche persuasive e strumenti tecnologici avanzati. Questa nuova forma di frode segna il passaggio da email generiche a strategie mirate, difficili da riconoscere e ancora più insidiose.

Indice degli argomenti

Dall'email sospetta al phishing 2.0

Il phishing è nato come pratica rudimentale di invio di una singola mail a migliaia di destinatari e ha a lungo funzionato in un'epoca in cui la consapevolezza sulla sicurezza informatica era pressoché inesistente, nonostante si presentasse spesso con un linguaggio sospetto e un link evidentemente malevolo. Oggi quel modello grezzo e facilmente riconoscibile è stato superato da una nuova generazione di attacchi: il **cosiddetto phishing 2.0, appunto.**

Phishing 2.0: il rapporto tra truffatori e vittime cambia volto

Si tratta di **un'evoluzione insidiosa che combina ingegneria sociale, tecnologie avanzate e una conoscenza profonda del comportamento umano.** In questo scenario, le tecniche di frode si sono affinate, diversificate e personalizzate, rendendo sempre più difficile distinguere tra ciò che è vero e ciò che è truffaldino.

Al cuore di questo cambiamento c'è una trasformazione radicale nel rapporto tra truffatori e vittime. **Il phishing 2.0 non si limita più a una semplice email generica, ma può assumere la forma di una telefonata, di un messaggio vocale generato da intelligenza artificiale**, di una chat su WhatsApp o addirittura di una richiesta di chiamata apparentemente legittima. Questo

approccio multidimensionale rende le minacce più difficili da rilevare e molto più efficaci. Le vittime non sono più casuali ma selezionate in modo mirato, sfruttando informazioni personali raccolte da fughe di dati, social network e altre fonti pubbliche o semi-private.

Quattro tecniche che ridefiniscono la frode digitale

In particolare, si sono sviluppate quattro tecniche particolarmente insidiose**: il vishing classico, l'uso di deepfake vocali, il callback phishing e il phishing via WhatsApp.** Ciascuna di queste modalità rappresenta un'evoluzione specifica della frode digitale, ed è già stata utilizzata con successo in diversi contesti internazionali.

Il vishing, tra continuità ed evoluzione

Il vishing, abbreviazione di "voice phishing", non è una tecnica nuova ma oggi è resa ancora più efficace. Si tratta di una telefonata da parte di un finto operatore bancario, di un impiegato di un'azienda tecnologica o di un'autorità pubblica, che avverte la vittima di una presunta anomalia: una transazione sospetta, un problema con il conto corrente, un attacco informatico in corso. Il truffatore, con tono rassicurante ma fermo, guida la vittima attraverso una serie di azioni che spesso includono il trasferimento di denaro, la condivisione di codici di accesso o l'installazione di software malevoli. Nonostante la sua semplicità, il vishing continua a colpire anche utenti esperti. Secondo un'indagine del Federal Trade Commission statunitense, nel solo 2024 gli attacchi in cui il metodo di contatto del truffatore è stata una telefonata hanno causato quasi 90 milioni di dollari di perdite negli Stati Uniti, mentre L'Espresso riporta a maggio di quest'anno che, nel 2024, l'85 % delle frodi bancarie in Italia ha avuto inizio con un contatto telefonico: voci gentili che si fingono operatori di banca, gestori telefonici o altri enti, spesso utilizzando numeri con prefisso italiano (+39), rendono la truffa molto credibile.

Deepfake vocali, la voce che inganna

La tecnica del vishing ha fatto un ulteriore passaggio evolutivo grazie alla possibilità di utilizzare una voce sintetica, o deepfake vocale. **Con gli strumenti di intelligenza artificiale, infatti, oggi è possibile clonare la voce di una persona con pochi secondi di registrazione** e questa tecnologia, pensata originariamente per scopi di accessibilità o doppiaggio, è stata rapidamente adottata anche dai cybercriminali. Il risultato è una nuova forma di ingegneria sociale, nella quale la vittima riceve una chiamata o un messaggio vocale da una voce indistinguibile da quella di un collega, un superiore, un familiare.

Nel marzo 2024, **il Financial Times ha riportato il caso della multinazionale asiatica Arup truffata per 25 milioni di dollari.** Il CFO, contattato telefonicamente da un presunto dirigente europeo, ha autorizzato un trasferimento urgente di fondi. La voce sembrava reale, il tono credibile. Solo dopo giorni l'azienda ha scoperto che si trattava di un deepfake vocale, generato a

partire da video pubblici e conferenze online. Il caso ha fatto il giro del mondo, dimostrando quanto la voce possa essere falsificata con precisione millimetrica.

Il callback phishing e l'inganno del numero di assistenza

Un'altra tecnica in crescita nell'attuale panorama della cybersicurezza è il cosiddetto "callback phishing": in questo scenario, la vittima riceve una e-mail apparentemente innocua, che simula ad esempio una fattura, un avviso di rinnovo di un servizio o un addebito sconosciuto. **A differenza del phishing classico, l'e-mail di per sé non contiene link o allegati malevoli, ma solo un numero di telefono da chiamare per chiarimenti.** Quando la vittima chiama, viene indirizzata a un call center gestito dai truffatori dove operatori convincenti conducono la conversazione verso l'installazione di malware o la condivisione di credenziali sensibili.

Un esempio particolarmente noto di callback phishing è rappresentato dalle campagne condotte dal gruppo Luna Moth (noto anche come Silent Ransom Group), attivo dal 2022. In questi attacchi, denominati "BazarCall", le vittime ricevevano e-mail che simulavano rinnovi di abbonamenti a servizi legittimi (come antivirus o piattaforme streaming), senza link o allegati dannosi, ma con l'invito a chiamare un numero di assistenza. Una volta contattato il call center, gli operatori portavano la vittima a installare software di accesso remoto come Zoho Assist o AnyDesk, che permettevano loro di ottenere il controllo completo del sistema. Questa tecnica, che unisce ingegneria sociale e abuso di strumenti legittimi, è stata usata per compromettere reti aziendali, esfiltrare dati sensibili e attuare estorsioni.

Phishing via whatsapp, la nuova frontiera della truffa

Infine, è stata rilevata una significativa esplosione del phishing via WhatsApp, una nuova frontiera della truffa digitale. Questo canale è diventato particolarmente diffuso tra i criminali grazie alla presenza dell'app in un numero elevatissimo di dispositivi, ma non solo. Ad aiutare nella buona riuscita della truffa è anche la sensazione di informalità che induce fiducia e all'uso di numeri apparentemente locali: i messaggi possono arrivare sotto forma di offerte di lavoro, avvisi di spedizione, promozioni esclusive o richieste d'aiuto da parte di contatti compromessi.

Nel luglio 2024, in Italia è emersa una nuova ondata di truffe su WhatsApp finalizzate alla divulgazione di offerte lavorative fasulle. I malintenzionati si fingevano aziende o recruiter, inviando messaggi che iniziavano con frasi come «Abbiamo ricevuto il tuo curriculum, aggiungici su WhatsApp per parlare di lavoro», innescando così una conversazione apparentemente legittima, che portava progressivamente a richieste di dati personali o accesso a conti bancari.

Come difendersi dal vishing classico

Di fronte a un panorama così mutevole, è essenziale sviluppare una nuova forma di consapevolezza. Le truffe del phishing 2.0 non sono solo un problema tecnologico ma soprattutto umano e proprio per questo motivo non è sufficiente installare software antivirus o aggiornare i sistemi per esserne

davvero protetti. A fare la differenza di fronte a questa categoria di minacce sono l'attenzione, la formazione e uno spirito critico attento ai dettagli. Ad esempio, nel caso del vishing classico, è utile ricordare che nessuna banca chiede mai codici o credenziali via telefono. Se si riceve una chiamata sospetta, meglio interrompere e richiamare il numero ufficiale della banca reperito autonomamente.

Riconoscere le voci sintetiche e verificarne l'autenticità

Per quanto riguarda i deepfake vocali, occorre prestare attenzione non solo alla voce, ma al contesto. Una richiesta inusuale di denaro, un'urgenza inspiegabile, un cambiamento di tono immotivato da parte di un collega dovrebbero attivare l'allarme e, in ambito aziendale, è buona prassi assicurarsi tramite un secondo canale di conferma in caso di richieste economiche significative, ad esempio via e-mail o chat aziendale certificata.

Evitare le trappole del callback phishing e di whatsapp

Nel caso del callback phishing, il primo campanello d'allarme è l'insistenza sulla necessità di chiamare un numero telefonico. In generale, è meglio evitare di rispondere a numeri sconosciuti o non verificati, soprattutto se associati a richieste di accesso remoto al computer. **Lo stesso vale per WhatsApp: anche se il messaggio proviene da un numero italiano, è fondamentale verificare l'identità del mittente prima di fornire qualsiasi informazione.**

Consapevolezza e spirito critico come difesa

In definitiva, il phishing 2.0 è una sfida complessa, che unisce vecchie strategie e nuove tecnologie per colpire nel punto più vulnerabile: la fiducia umana. Ma proprio la consapevolezza può diventare il primo antidoto. In un mondo dove le voci possono essere finte, i numeri telefonici mascherati e i messaggi confezionati con cura maniacale, l'unico vero strumento di difesa resta la nostra capacità di dubitare, riflettere e verificare.