Paolo Attivissimo

Yuka, l'app-semaforo per cibi e cosmetici aiuta ma va letta bene

Yuka è un'app gratuita molto diffusa che assegna una valutazione a cibi e cosmetici: basta inquadrare con la fotocamera del telefonino il codice a barre di un prodotto per ottenere un bollino colorato che rappresenta il punteggio di quel prodotto.

L'app assegna questo punteggio sulla base di numerosi criteri: per gli alimenti, per esempio, considera prima di tutto gli ingredienti e poi la loro qualità nutrizionale, la presenza di additivi considerati a rischio e la "natura biologica", ossia la presenza dell'etichetta bio europea.

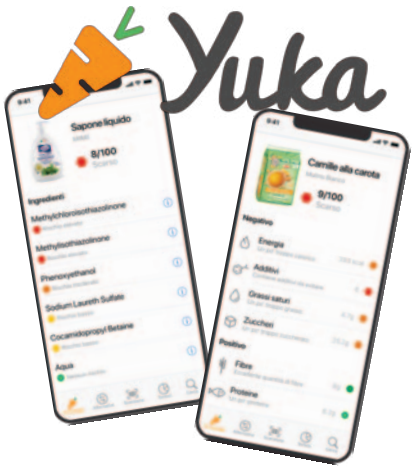
La società che la gestisce, la parigina Yuca SAS, dichiara di non ricevere finanziamenti dalle industrie produttrici e di mantenersi esclusivamente attraverso la versione a pagamento dell'app, che costa 15 euro all'anno e offre alcuni vantaggi extra ai suoi utenti (per esempio avvisi per prodotti non adatti a diete vegetariane o vegane oppure senza glutine o lattosio), e la vendita di un libro e di un calendario. L'app, inoltre, non contiene pubblicità.

Yuca SAS afferma di basare i propri punteggi esclusivamente su dati scientifici, che elenca dettagliatamente, con l'intento di informare i consumatori sul contenuto di quello che comprano, e la sua popolarità ha indotto molte aziende a cambiare gli ingredienti dei prodotti alimentari e cosmetici per evitare il "semaforo rosso" dell'app, che sconsiglia un prodotto e propone un'alternativa con un punteggio migliore. La catena di distribuzione francese Intermarché, per esempio, nel 2019 ha annunciato che avrebbe cambiato la composizione o il confezionamento di ben 900 prodotti per migliorare i loro piazzamenti in Yuka.

Da tutti questi punti di vista, insomma, usare l'app Yuka è utile e consigliabile, ma è indispensabile saperla usare con consapevolezza e senza fermarsi alla semplice indicazione colorata, come viene invece istintivo fare per esempio quando si devono valutare tanti prodotti durante la spesa al supermercato. Il sistema a semaforo dell'app, infatti, tende a semplificare troppo e a nascondere le complessità, portando a volte a indicazioni fuorvianti.

Per esempio, il colore assegnato a un alimento si basa per il 60% sulla qualità nutrizionale (metodo Nutri-Score), al quale Yuka applica fattori correttivi non specificati, per il 30% sulla presenza di additivi e per il 10% sulla qualità bio. La scelta di queste percentuali è completamente arbitraria e priva di basi scientifiche. Perché proprio queste cifre così tonde e non delle altre? Inoltre i criteri di Yuka possono spingere le aziende a offrire cibi che hanno un punteggio molto alto nell'app ma un basso contenuto nutrizionale (sale, burro e zucchero, per esempio, sono considerati "negativi") e portare gli utenti verso diete sbilanciate.

Per i cosmetici, invece, la valutazione si basa "sull'analisi dell'insieme degli ingredienti del prodotto": una frase molto ambigua. Questa ambiguità e arbitrarietà si abbinano al fatto che l'app non tiene conto delle dosi degli ingredienti, per cui un cosmetico che contiene solo tracce minime di una sostanza ritenuta a rischio (per esempio un conservante necessario per evitare le muffe) può ricevere lo stesso bollino rosso di un prodotto che ne contiene grandi quantità, e siccome l'app mostra normalmente solo il bollino peggiore (per vederli tutti bisogna far scorrere in su la scheda informativa), un cosmetico che contiene tanti ingredienti ottimi ma una quantità anche minima di un solo ingrediente che Yuka considera a rischio può sembrare peggiore di uno che contiene solo ingredienti mediocri o scadenti ma nessuno ottimo. Stabilire la qualità e la sicurezza di un prodotto è una questione complessa, che non si può ridurre a un semplice bollino rosso, arancione, giallo o verde. Yuca SAS lo sa bene, e infatti nel contratto di licenza dell'app specifica che "l'utente deve essere cosciente della complessità dei campi della nutrizione, della cosmetica e dell'analisi ambientale" e che l'app "fornisce una prima analisi… ma non garantisce una salute migliore all'utente". Inoltre il punteggio, dice Yuca SAS, "costituisce una opinione basata sulle informazioni presentate sul prodotto". La parola chiave è "opinione": in altre parole, l'azienda non si assume alcuna responsabilità e offre solo i propri pareri soggettivi.Usata con giudizio e conoscendone le limitazioni, Yuka può essere un assistente pratico per ricordare se un certo ingrediente è consigliabile o sconsigliabile e per rendere più leggibili gli ingredienti, che purtroppo le etichette riportano sempre più spesso in caratteri microscopici. Ma un semplice semaforo non può sostituire un consumatore consapevole e ben informato.



Consigli ACSI

- Non fermatevi al primo bollino indicato da Yuka per un prodotto: fate sempre scorrere verso l'alto la sua scheda informativa per vedere i dettagli della valutazione.
- Tenete conto del fatto che gli ingredienti dei prodotti sono sempre indicati sulla loro etichetta in ordine di quantità decrescente; questo compensa le limitazioni di Yuka.
- Se fate la spesa con i vostri bambini, provate a fare usare a loro Yuka: li coinvolgerete nel processo di scelta degli acquisti e cominceranno a conoscere i nomi degli ingredienti dei prodotti.

Paolo Attivissimo

Difendersi dalle **truffe nelle prenotazioni di alloggi** su Internet

Si avvicina la stagione delle vacanze e molte persone stanno facendo prenotazioni via Internet su siti come Tripadvisor e Booking, mentre i criminali informatici stanno preparando trappole sempre più sofisticate che riguardano questi servizi. Per evitare di perdere soldi e trovarsi con la vacanza rovinata conviene conoscere le tecniche di raggiro più usate.

Nello schema classico, il truffatore crea una falsa inserzione sui siti di viaggi: una pagina che illustra dettagliatamente un alloggio che in realtà non gli appartiene o non esiste del tutto. Il criminale lo offre a un prezzo particolarmente allettante e poi aspetta che arrivino le prenotazioni. Quando arrivano, manda a ciascun aspirante cliente via WhatsApp un link a un finto "modulo di caparra", che ha lo stesso aspetto grafico del sito di viaggi autentico ma è in realtà un sito gestito dal truffatore, nel quale la vittima è invitata a immettere i dati della propria carta di credito, credendo di pagare la caparra. In questo modo il truffatore ottiene i dati della carta e li usa per sottrarre soldi alla vittima.

Ma c'è anche una versione più sofisticata e insidiosa di questo tipo di truffa: la vittima fa una prenotazione perfettamente regolare, presso un albergo realmente esistente, passando da un sito legittimo come Booking o Tripadvisor o rivolgendosi direttamente al sito autentico dell'albergo, e poi riceve un messaggio su WhatsApp da una persona che ha lì un account Business e si presenta come amministratore dell'alloggio. Questa persona riepiloga i dettagli della prenotazione e chiede molto educatamente di confermarli. La conversazione ispira particolare fiducia, perché in questo caso è normale presumere che chi sa questi dettagli sia il legittimo gestore.

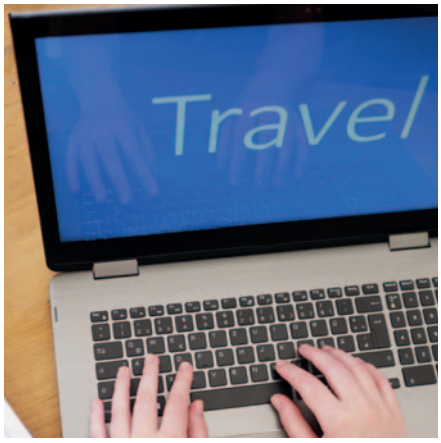
Se si risponde alla richiesta, la conversazione via WhatsApp prosegue con una garbata richiesta di caparra o di "verifica" della carta di credito, tramite un link che come nel caso precedente porta a un sito gestito dal truffatore. Anche qui la truffa si conclude con il saccheggio del conto della carta della vittima.

Il funzionamento del primo metodo è abbastanza intuitivo, visto che la vittima ha immesso i propri dati direttamente nella pagina falsa del malvivente; ma come fa invece il truffatore a sapere della prenotazione nel secondo metodo, visto che i dati della vittima sono effettivamente custoditi presso il sito di viaggi o quello dell'albergo?

La risposta più probabile, secondo le segnalazioni dei servizi antifrode in vari paesi europei, è che l'albergo abbia subìto, senza accorgersene, un'intrusione informatica che ha permesso ai truffatori di accedere di nascosto all'elenco delle prenotazioni; il cliente non ha colpa. Se per esempio i truffatori sono riusciti a rubare con l'inganno la password di gestione del conto Tripadvisor o Booking dell'albergo, possono leggere tutti i dettagli delle prenotazioni e usarli per contattare chi le ha fatte e tentare di frodarli con buone probabilità di successo, perché molte persone non arriveranno a immaginare che un truffatore possa conoscere tutti i particolari dei viaggi che hanno riservato e quindi si fideranno della presa di contatto.

Difendersi da questi raggiri richiede attenzione: bisogna guardare se il prefisso telefonico internazionale di chi ci contatta è diverso da quello della località prenotata, se viene chiesto di cliccare su un link il cui nome non corrisponde a quello del sito di viaggi (ma magari gli somiglia molto, come per esempio booking-payments.com) e soprattutto insospettirsi se arriva una richiesta di comunicare su WhatsApp o altri canali differenti da quelli ufficiali. Nel dubbio è molto importante non farsi prendere dalla foga e dalla voglia di concludere in fretta i preparativi di viaggio: i truffatori contano proprio su questo.

Ovviamente anche i gestori di alloggi devono fare la propria parte evitando le intrusioni: il Centro nazionale per la cibersicurezza ha segnalato recentemente che diversi dipendenti di hotel hanno ricevuto via mail richieste di presunti ospiti che cercano di convincerli ad aprire un link con vari pretesti. I dipendenti che cadono nella trappola permettono ai malviventi di installare un virus informatico che può dare accesso agli account dell'hotel per compiere truffe.



Se vi accorgete in tempo di un tentativo di truffa oppure ne siete stati colpiti, potete segnalarlo ad Antiphishing.ch e al Centro nazionale per la cibersicurezza presso www.ncsc.admin.ch. Questo aiuterà le autorità a bloccare rapidamente il sito dei truffatori.

Consigli ACSI

- Rifiutate qualunque richiesta di informazioni o di pagamento che arrivi da canali, indirizzi di mail o numeri di telefono diversi da quelli indicati nel sito dove avete prenotato.
- Non cliccate mai su link ricevuti nei messaggi, specialmente sul telefonino.
- Usate, se possibile, una carta di credito prepagata, che limita il rischio economico.
- Diffidate delle offerte a prezzi troppo convenienti.

Paolo Attivissimo

Profili professionali ticinesi su Facebook rubati per terrorismo

Sono in gran numero, anche in Ticino, le piccole aziende e i professionisti di vari settori che creano un profilo Facebook per farsi conoscere o anche semplicemente per farsi trovare e comunicare con i clienti. Facebook offre servizi appositi, come la "modalità Professionale" o gli account aziendali, ma non tutti li sfruttano, preferendo la familiarità e la semplicità di un normale profilo (anche se questo viola le regole di Facebook). Ma troppa semplicità può comportare un danno molto sorprendente: quello di diventare disseminatori di messaggi terroristici.

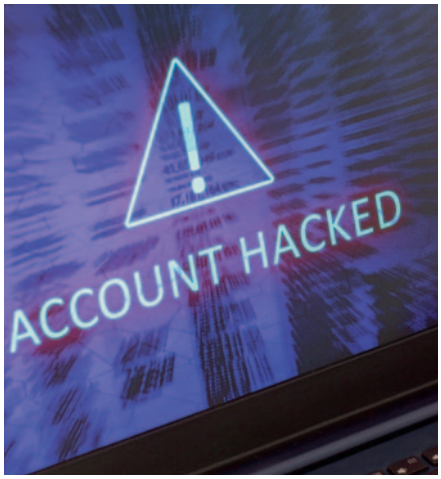
Di recente, infatti, ho ricevuto numerose richieste di soccorso di persone che hanno perso improvvisamente l'accesso al proprio profilo Facebook, personale o professionale, e lo hanno visto trasformarsi in pagine di promozione di siti di gioco d'azzardo o pornografia, e questo è purtroppo abbastanza normale. Ma in alcuni casi, anche locali, i profili professionali sono stati rubati per pubblicare messaggi di sostegno a varie ideologie estremiste e a organizzazioni legate al terrorismo.

Perdere il controllo di un profilo social personale è già molto fastidioso, perché si perdono i contatti con gli amici online; perdere l'accesso al proprio profilo professionale è un disagio ben maggiore, perché si interrompono le comunicazioni con i clienti esistenti, non si possono ottenere clienti nuovi, e c'è inevitabilmente un danno d'immagine per la propria attività. Se poi addirittura il profilo ospita messaggi di odio o istigazione al terrorismo, ci possono essere anche conseguenze legali molto spiacevoli. Evitare questi incidenti è possibile, ma richiede prima di tutto un cambiamento di atteggiamento: moltissimi utenti pensano che il loro profilo non possa far gola a nessun malintenzionato e quindi non ritengono opportuno proteggerlo approfonditamente. Ma gli incidenti informatici che mi sono stati segnalati dimostrano che i ladri di profili attaccano chiunque, dalla docente al parrucchiere al fotografo. Il loro criterio non è la visibilità o l'importanza del profilo, ma la facilità maggiore o minore di rubarlo. Pubblicano il loro spam, o i loro messaggi di odio, ovunque riescano. Questo vuol dire che qualunque profilo è per loro un bersaglio appetibile. Per proteggere il proprio profilo da questi ladri opportunisti si comincia dalle basi: si usa una password differente da quella usata per tutti gli altri servizi di Internet e difficile da indovinare (niente date di nascita o nomi dei figli o nipoti) e si attivano la cosiddetta "autenticazione a due fattori" e i "codici di recupero". Le istruzioni sono facilmente reperibili in Google o in www.facebook.com/help.

Già questo scoraggia la maggior parte dei ladri, ma non basta: bisogna anche fare attenzione a messaggi con richieste di verifica password apparentemente provenienti da Facebook ma in realtà inviate da aspiranti ladri. Non è difficile: basta ricordare che Facebook non vi chiederà mai la password in un messaggio.

Un altro trucco usato dai ladri è offrire app di gioco o barre strumenti (le cosiddette "estensioni dei browser") in regalo, che in realtà servono per rubare le password: conviene ignorare queste offerte.

I profili professionali e aziendali vengono rubati spesso attaccando il punto più debole, che è il profilo personale di chi li gestisce, solitamente meno protetto. Il ladro entra da lì e prende rapidamente il controllo di tutto, cambiando mail e numero di telefono. Le misure che ho descritto sopra vanno quindi applicate anche al profilo personale. Per i profili personali e professionali (ma non aziendali) c'è da poco anche una protezione ulteriore: si chiama Meta Verified. Offre assistenza diretta da una persona di Meta (l'azienda che gestisce Facebook), il monitoraggio attivo del profilo contro i furti di identità e una sorta di bollino di autenticazione che permette agli altri di sapere che il vostro profilo è reale e autenticato e non appartiene a un impostore. Richiede però l'invio di un'immagine di un documento di identità a Meta e un canone mensile di circa 14 franchi. Per chi è abituato a Facebook gratuito può sembrare un prezzo notevole, ma il costo di un furto irrimediabile di un profilo, specialmente se usato per lavoro, è ben più alto.



Consigli ACSI

- Conviene sempre denunciare in Polizia un furto di profilo social, per mettersi al riparo da eventuali conseguenze legali di qualunque cosa pubblicata sul vostro profilo dai ladri.
- Verificate di aver immesso nel profilo la vostra vera data di nascita, altrimenti non corrisponderà a quella sul documento di identità se lo mandate a Meta. Attenzione: chi ha esagerato la propria età in passato perché troppo giovane rischia il blocco del profilo.
- Invece degli SMS di verifica, usate le app di autenticazione (come Google Authenticator o Twilio Authy, gratuite).
- In caso di furto, non rispondete alle mail di avviso inviate da Facebook: le vostre risposte non verranno lette. Consultate invece l'assistenza clienti nell'app di Facebook.