Ischia: Se la frode ci viene recapitata dalla posta elettronica…

I mille modi di carpire importanti dati personali mediante fantomatiche vincite, aperture di conto, intimazioni più o meno inquietanti

L'unica vera difesa contro i tentativi di truffa via email è la conoscenza e quindi la prevenzione dei pericoli che si corrono on-line. Avviene con sempre maggiore frequenza, ma non per questo è meno temibile. Un tempo neanche esistevano i termini per definirlo, né esistevano gli strumenti elettronici per combatterlo, mentre oggi tutti i programmi antivirus e gli stessi software di posta elettronica prevedono soluzioni (non sempre efficaci) per arginare un fenomeno che sta raggiungendo dimensioni molto allarmanti:

il phishing.
Fino a qualche tempo fa le frodi via email erano piuttosto rare: tutt'al più la nostra casella di posta elettronica veniva spesso riempita da "spam", la cosiddetta "posta spazzatura", spesso indicata anche come "junk-mail", che traduce letteralmente l'espressione. È interessante conoscere l'origine del termine "spam", che risale ad uno sketch comico all'interno di una commedia televisiva britannica, il Monty Python's Flying Circus, durante il quale la cameriera di un locale insisteva nel proporre agli ospiti tutti i piatti che contenevano Spam, ossia un tipo di carne di prosciutto di maiale in scatola. Quanto più i clienti cercavano di rifiutare questi tipi di portate, tanto più la camera insisteva nel proporli, rendendo paradossale la comunicazione e, per contro, decisamente efficace la satira verso la pubblicità vera di quel prodotto, che era in effetti asfissiante. Etimologia perfetta, dunque, per identificare la posta indesiderata, che tentava di vendere prodotti di ogni genere ad ogni costo, un po' come succedeva un tempo con la posta tradizionale. Fondamentale però è la differenza rispetto ai rischi, poiché lo spam o junk-mail era ed è innocuo dal punto di vista della truffa: è semplice pubblicità, per quanto non richiesta e fastidiosa.
Al contrario, la frode elettronica, il "phishing" appunto, dannosa lo è, eccome. Perché si basa sull'inganno verso il ricevente, a cui mira a sottrarre l'identità (di solito bancaria o postale, oppure quella relativa alle carte di credito e così via), per poterne poi fare un uso fraudolento. Ma come avviene di solito il phishing? Nel modo apparentemente più innocuo: mediante l'invio di messaggi email da falsi mittenti (di solito istituti bancari, Poste Italiane, istituti che emettono carte di credito, grandi portali di vendita on-line), in cui si richiede di accedere al proprio account mediante il link indicato all'interno del corpo della mail. Le ragioni più usate per questi messaggi vanno dal tono tranquillo con cui si comunica che bisogna "attivare la procedura per usufruire dei vantaggi esclusivamente riservati al beneficiario", al tono festoso con cui si certifica l'avvenuta vincita di importi spropositati di danaro, riscuotibili mediante la conferma attraverso il link, al tono minaccioso con cui si intima di entrare subito nell'area riservata, sempre mediante il

link proposto, per “ripristinare immediatamente il proprio conto corrente, che intanto è stato chiuso” perché non l’abbiamo attivato tramite la procedura disponibile” sul famigerato link! Cosa succede se l’ignaro utente clicca sull’infame link? Succede che si accede APPARENTEMENTE alla pagina della banca, delle Poste e così via, mentre in realtà si stanno fornendo i propri dati (user name, password, numero di conto e quant’altro) ai truffatori, che potranno così utilizzarli per compiere operazioni fraudolente, di cui purtroppo si viene a conoscenza quando è già tardi per bloccarle.
A livello mondiale la lingua più utilizzata nel phishing è ovviamente l’inglese, seguito però, per nostra sfortuna, dall’italiano, che sorprendentemente si è imposto su idiomi molto più parlati al mondo, come lo spagnolo, il cinese e l’arabo. E dire che il livello d’italiano di questi messaggi era decisamente scadente fino a poco tempo fa: era evidente che i truffatori ricorrevano ai traduttori automatici, incapaci di tradurre in modo coerente e corretto, per cui il testo risultava talmente ridicolo da non essere neanche degno di considerazione. Ora invece spesso sono scritti in italiano corretto e strutturati in modo da sembrare seri e affidabili.
Ultimo gradino nella scala di meschinità e grettezza dei tentativi di frode on-line è quello che include le minacce di morte. In realtà, anche in questi casi lo scopo è sempre e solo quello di appropriarsi dei dati bancari del malcapitato, a cui si offre di risparmiargli la vita se rivelerà le informazioni riservate legate alla sua carta di credito e simili. Qui si lavora completamente sul panico che si origina da minacce di questa portata, entrando pienamente nell’ambito del terrorismo psicologico, oltre che in quello già evidente della truffa.
Esiste un solo modo per evitare di cadere in queste trappole: affidarsi intanto ad un buon antivirus che possegga un forte filtro anti-spam (poiché questo bloccherà tutto ciò che gli risulta essere ALMENO spam), controllare che, al contrario, nella casella di Posta Indesiderata non sia finita invece qualche email da mittente valido e non fidarsi comunque a priori delle email che i vari filtri hanno lasciato passare. Questo significa che, tra tutte le email scaricate nella casella di Posta in Arrivo, è saggio aprire solo quelle provenienti da fonte sicura, il che non vuol dire che basterà leggere un mittente ben noto, come il nome di una banca, di un portale di commercio on line o di un istituto emittente carte di credito, per aprire un messaggio. Al contrario, questo dev’essere un indizio che mette in guardia, perché quasi sicuramente si tratta di phishing. Solo nel caso in cui abbiamo realmente in essere un rapporto con il mittente, possiamo considerare l’idea di validità del messaggio, verificandone però direttamente la veridicità. Come? Telefonando, se in orari d’ufficio, oppure aprendo un NUOVO MESSAGGIO di posta elettronica, inserendo l’indirizzo a noi già noto e verificato, per chiedere conferma riguardo al messaggio ricevuto, di cui NON si copieranno e inseriranno delle parti nella nuova email, bensì se ne spiegheranno brevemente i contenuti.
In tutti gli altri casi, ossia quando riceviamo messaggi da sedicenti istituti bancari o di credito o ancora portali ed enti vari, soprattutto quando ci comunicano che abbiamo vinto un premio grazie ad un concorso a cui non abbiamo mai partecipato, o quando si verificano ricatti (“se non accedi alla tua area riservata, il tuo conto sarà chiuso o non sarà mai attivato”), minacce o anche quando semplicemente si viene invitati ad acquistare farmaci miracolosi o materiale più o meno pornografico, NON bisogna mai aprire i messaggi, o, se lo si è fatto, mai cliccare sui link o sugli allegati, perché, se ci andrà “bene”, saremo inondati da virus, spyware e cavalli di Troia.
Per ulteriori info e soprattutto per tutelarsi: http://www.anti-phishing.it/
Fidarsi è bene; non fidarsi, su internet, è oggi indispensabile.