Natale e privacy: raccomandazioni per la data protection

DURANTE LE FESTE, OGNI ANNO, SI MOLTIPLICANO LE MINACCE PER LA PRIVACY. I RISCHI PIÙ COMUNI DERIVANO SIA DA FONTI ESTERNE, QUALI CYBER CRIMINALI CHE PUNTANO SULLO SPIRITO NATALIZIO PER SFERRARE ATTACCHI DI INGEGNERIA SOCIALE, SIA DALLA MANCATA SENSIBILIZZAZIONE AL TEMA DELLA DATA PROTECTION.
PROPRIO AL FINE DI PROMUOVERE LA CULTURA DELLA PROTEZIONE DEI DATI PERSONALI ED INCREMENTARE LA CONSAPEVOLEZZA DEI CITTADINI, L'AUTORITÀ GARANTE HA PUBBLICATO I SUGGERIMENTI PER PROTEGGERE "LA PRIVACY SOTTO L'ALBERO". COSA SAPERE PER TUTELARSI?

Federico Corti
Dicembre 22, 2023
Scarica PDF dell'articolo

PHISHING E INGEGNERIA SOCIALE

L'elenco di raccomandazioni del Garante parte, non a caso, dalla minaccia più frequente durante le festività. Si tratta degli **attacchi di phishing**, spesso volti a veicolare ransomware, ovvero virus informatici in cui gli attori delle minacce prendono il controllo delle risorse di un obiettivo e chiedono un riscatto in cambio della restituzione della disponibilità di tali risorse.

L'incremento di operatività dei cyber criminali nei periodi festivi, è un trend che si ripete ormai da diversi anni. Durante le vacanze natalizie, infatti, gli investimenti e le azioni volte ad incrementare il livello di cybersecurity sono al minimo, così come il personale attivo ed operante in azienda. Allo stesso modo, anche i servizi di supporto informatico esterni sono ridotti all'indispensabile. Sfruttando questi **momenti di maggiore vulnerabilità** di enti ed imprese, abbiamo assistito all'ascesa del **ransomware "Cl0p"** che, nel corso del 2023, è emerso come **minaccia dominante nel panorama dei crimini informatici**, detronizzando di fatto il precedente leader, "LockBit". I gruppo dietro Cl0p è riuscito a infiltrarsi e a compromettere centinaia di organizzazioni, proprio grazie ad attacchi su larga scala condotti durante le occasioni festive.

Akamai Security Research, centro che raggruppa ricercatori, ingegneri, strateghi e data scientist di livello mondiale, inoltre, ha rilevato il diffondersi di un **kit di phishing** altamente sofisticato e molto attivo in occasione delle festività natalizie dello scorso anno. Il kit, facendo leva sulla reazione emotiva delle vittime, agiva **imitando le manovre di marketing di note aziende, promettendo un premio in cambio dell'inserimento dei propri dati personali**.

Le **comunicazioni "esca"** possono essere molto diverse fra loro: lettere di auguri con allettanti inviti ad agire (soprattutto nei periodi festivi); comunicazioni relative all'invio di pacchi e al tracciamento delle spedizioni; oppure offerte (quasi) incredibili con sconti su viaggi, abbigliamento, buoni e gift card, oggetti di vario genere, che è possibile ottenere solo a condizione di effettuare determinate azioni. Mediante tali messaggi viene richiesto alle vittime di rispondere a sondaggi o questionari, di fornire dati personali o bancari, di cliccare su appositi link, di aprire allegati, etc. Tutte queste azioni consentono ai criminali informatici di perseguire i propri scopi malevoli (il furto di dati personali e bancari, il furto di credenziali di autenticazione, l'estorsione mediante ransomware, etc.).

Nell'eterogeneo panorama di esche e di relativi vettori (ricordiamo, infatti, che non esiste solo il phishing via mail ma anche il c.d. "smishing", condotto tramite SMS truffa, o il c.d. "vishing", condotto mediante telefonate ingannevoli), vi sono alcuni specifici elementi che accomunano questa tipologia di minacce:

1. fanno leva sull'**errore umano**;
2. sfruttano le **emozioni** e lo "**spirito natalizio**";
3. sono **sempre più credibili** e personalizzate, grazie all'uso dell'Intelligenza Artificiale;
4. mirano a ottenere **l'accesso a informazioni o servizi** per generare profitti illeciti.

Il Garante raccomanda quindi, in caso di ricezione di comunicazioni sospette:

- di **evitare** di compiere **azioni istintive**: meglio attendere che la naturale reazione emotiva e la curiosità del momento passino;
- di **riflettere** se è il caso di rispondere o compiere le azioni richieste, tanto più se il mittente è sconosciuto;
- di **verificare**, ad esempio, se il messaggio proviene da un sito affidabile, se effettivamente sono in corso campagne promozionali o se ci sono notizie online sulla serietà del venditore, e magari cercare di reperire i contatti ufficiali (telefono, e-mail, etc.) per chiedere conferma della veridicità delle offerte ricevute;
- se il messaggio riguarda il tracking dei pacchi o l'aggiornamento di un ordine effettuato su siti di e-commerce online, di fare sempre **riferimento alla piattaforma** su cui sono stati eventualmente effettuati degli acquisti o al sito dello spedizioniere;

se il messaggio proviene da persone che conosciamo ma ci appare anomalo, di provare a contattarle attraverso altri canali per verificare l'effettiva identità del mittente.

PAGAMENTI ONLINE E GESTIONE DEI CONTI

Altre minacce alla riservatezza dei dati tipiche dei periodi festivi, possono derivare dall'utilizzo di **servizi online** per fare regali o per prenotare vacanze.

Il Garante ricorda che:

- in caso di acquisti online è sempre meglio **usare carte di credito** prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto corrente o della carta di credito;
- è utile **impostare avvisi** (*alert*) per essere a conoscenza in tempo reale delle transazioni che avvengono sul conto o sulla carta di credito e accorgersi di eventuali addebiti non autorizzati per poter intervenire rivolgendosi subito alla propria banca o al gestore della carta;
- è importante **controllare l'indirizzo Internet dei siti** su cui si fanno pagamenti online: in particolare, verificare se il sito web indicato corrisponde effettivamente all'azienda che dovrebbe gestirlo;
- è importante **controllare se vengono rispettate le procedure di sicurezza** standard per i pagamenti online (ad esempio, la URL – cioè l'indirizzo – del sito deve iniziare con "https" e avere il simbolo di un lucchetto).

MINACCE DALLE APP PER SMARTPHONE

Le statistiche relative ai download di applicazioni mobile, sui principali store, evidenziano un incremento netto durante i periodi festivi. I servizi richiesti sono di diverso tipo: dalle app per creare e inviare cartoline di Natale, a quelle per avere uno screensaver natalizio, sino a servizi di e-commerce e giochi. La prima regola di sicurezza essenziale, in questi casi, è quella di **fare affidamento esclusivamente alle app presenti sui market store ufficiali**.

Il Garante, inoltre, raccomanda di:

- **leggere con attenzione le descrizioni delle app** (se, ad esempio, nei testi sono presenti errori e imprecisioni, c'è da sospettare);
- **consultare eventuali recensioni** di altri utenti nell'uso di una determinata app o di una piattaforma per verificare se sono segnalati problemi riguardanti la sicurezza dei dati;
- **evitare che i minori possano scaricare film, app o altri prodotti informatici** da soli, magari impostando limitazioni d'uso sul loro smartphone o tablet, oppure creando profili con impostazioni d'uso limitate se usano quello dei genitori.

DIFFUZIONE ILLECITA DI FOTO E VIDEO

Un'altra minaccia per la privacy attiene alla **realizzazione**, e conseguente **diffusione sui social, di foto e video realizzate durante pranzi, cene ed eventi natalizi**. La diffusione di contenuti personali sul web è sempre un trattamento molto delicato, in particolar modo quando riguarda soggetti minori di età (pensiamo, ad esempio, alla pubblicazione delle foto di una recita di fine anno).

Il Garante raccomanda, quindi, di:

- Accertarsi, prima di pubblicare online foto o video in cui compaiono altre persone, che queste siano d'accordo, soprattutto se si inseriscono anche tag con nomi e cognomi.

In caso di riprese di bambini e ragazzi occorre adottare alcune accortezze ulteriori:

- Evitare di postare le foto sui social network;
- (se proprio indispensabile postare foto di minori sul web) richiedere il consenso di chi esercita la potestà genitoriale;
- (se proprio indispensabile postare foto di minori sul web) attivare l'impostazione che le rende visibili ai soli "Amici". Questo in considerazione del fatto che le immagini dei minori potrebbero essere visualizzate e scaricate anche da malintenzionati;
- (se proprio indispensabile postare foto di minori sul web) rendere irriconoscibile il viso (ad esempio, utilizzando programmi di grafica per "pixellare" i volti, semplici da usare e disponibili anche gratuitamente online, o posizionando semplicemente sopra una "faccina" emoticon).

DIFFUSIONE DI ALTRE INFORMAZIONI PERSONALI

Come anticipato, la diffusione è sempre un trattamento molto delicato. Anche quando non riguarda fotografie e videoriprese, è essenziale **prestare attenzione ai contenuti che pubblichiamo su web e social**. Ad esempio, informazioni che possono rivelare per quanto tempo si sarà assenti e in quali giorni potrebbero essere utili a eventuali malintenzionati.

In questo caso l'Autorità ricorda di:

- **evitare sempre di diffondere online informazioni molto personali** come l'indirizzo di casa o le foto del proprio appartamento. Da queste ultime, in particolare, potrebbero essere ricavate indicazioni sulle misure di protezione (tipologia delle serrature e delle finestre, presenza di telecamere, allarmi o inferriate, ecc.) oppure sulla presenza in casa di oggetti di valore (tv, quadri, etc.);
- **non lasciare online indicazioni** (anche indirette) **sul fatto che si è partiti** lasciando incustodito il proprio mezzo di trasporto personale (auto, moto, scooter, etc.), magari fornendo anche involontariamente informazioni su dove si trova.

OCCHIO A DISPOSITIVI SMART E DOMOTICA

Se si parte per le vacanze ed in casa sono presenti prodotti e sistemi domotici è bene ricordarsi che tali dispositivi possono esporre ad attacchi informatici, virus e malware. Lo stesso discorso si applica ai giocattoli smart, ovvero giocattoli intelligenti e interattivi ma in grado di raccogliere e trattare dati personali degli utilizzatori, piccoli e grandi. Tutti questi oggetti necessitano di attenzione.

Il Garante ricorda di:

- **adottare misure di protezione adeguate**, quali password forti e aggiornamenti software / patch di sicurezza;
- prima di partire **spegnere o disconnettere i dispositivi smart** non indispensabili;
- per i sistemi smart che restano operativi in vacanza, si possono eventualmente impostare **sistemi di *alert*** per controllare a distanza il loro funzionamento e monitorare anche lo stato della propria abitazione.

SERVIZI WI-FI IN VACANZA

Giunti in albergo o al ristorante, è spesso possibile accedere a servizi di **connessione Wi-Fi**. Tali servizi potrebbero **non** essere **adeguatamente protetti** ed esporre i dispositivi degli utenti a virus, software malevoli o intrusioni esterne (c.d. attacchi "man in the middle") da parte di malintenzionati a caccia di dati personali.

L'Autorità Garante suggerisce, qualora non si sia certi degli standard di sicurezza adottati, di:

- **evitare di accedere ai servizi online** che richiedono credenziali di accesso (ad esempio, la propria webmail, i social network, il conto corrente, etc.) o fare acquisti online con la carta di credito.

PRIVACY E DRONI IN VACANZA

Infine, anche **l'uso di droni in vacanza** (ad esempio sulle piste da sci), necessita di alcune accortezze per non invadere gli spazi personali e la riservatezza delle altre persone.

Il Garante raccomanda di:

- informarsi bene sulle **regole previste dall'ENAC**;
- **evitare di invadere gli spazi** personali e l'intimità delle persone;
- diffondere le immagini solo se i **soggetti ripresi non** sono **riconoscibili**;
- **evitare di riprendere e diffondere** immagini che contengono **dati personali** come targhe di macchine, indirizzi di casa, etc.

LA PRIVACY NON VA IN VACANZA

Come abbiamo visto, le principali minacce alla privacy, che caratterizzano il periodo natalizio, derivano dall'uso di dispositivi digitali, applicativi e social network senza le dovute accortezze.

La prima linea di difesa è sempre la **consapevolezza nell'uso di tali tecnologie e dei rischi** che ne derivano. Per tale ragione, è essenziale attenersi alle raccomandazioni del nostro Garante e, soprattutto, non abbassare la guardia: **la privacy non va in vacanza!**