MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Festeggia in Sicurezza

Consigli per evitare truffe informatiche nel periodo natalizio

Sommario

Cosa troverai in questa brochure

Introduzione

Durante le festività natalizie, secondo un'analisi condotta dal CSIRT (*Computer Security Incident Response Team*) Italia, si assiste periodicamente ad un **incremento degli attacchi informatici.** Infatti, a seguito della maggiore propensione degli utenti ad effettuare gli acquisti online, questo periodo è propizio per la diffusione di **malware** derivanti dall'interazione con e-mail fraudolente, messaggi truffaldini, etc.

Lo scambio di auguri e l'acquisto online di regali porta milioni di persone **ad interagire con messaggi e ad effettuare transazioni bancarie digitali**, spesso non adottando il giusto livello di attenzione ed esponendosi così a potenziali conseguenze dannose.

In tale periodo i criminali informatici creano **falsi siti e-commerce** che, imitando quelli legittimi, spingono gli utenti ad inserire i propri dati personali, esponendoli a **furti di identità** e **frodi bancarie**.

Natale sotto attacco

236 Gli eventi cyber verificatisi nel mese di Dicembre 2024 in Italia.

+38% La percentuale di aumento di eventi cyber rispetto il mese di Novembre 2024.

Gli auguri che non ti aspetti

Attenzione ai messaggi promozionali!
I messaggi di auguri via e-mail, SMS che recapitano un **codice sconto** in occasione delle festività natalizie, **possono nascondere malware**.

Come ti possono colpire?
Basta un **click** su un'immagine, un allegato o un link, e il gioco è fatto! Una volta eseguito, il **malware** compromette la **sicurezza** dei tuoi **dati** e delle tue **informazioni personali**.

Proteggi la tua sicurezza online!
In un periodo così delicato, è essenziale adottare **buone pratiche di sicurezza informatica**. Non lasciare che un semplice augurio si trasformi in un problema per la tua sicurezza digitale!

Fonte: ACN – Operation Summary Dicembre 2024

Quali sono i rischi?

Rischi

01 Manipolazione Psicologica

Durante il **periodo natalizio**, i criminali informatici sono soliti avvalersi delle tecniche di ingegneria Sociale (**Social Engineering**) per sferrare attacchi informatici, che fanno leva sulla **manipolazione psicologica** finalizzata ad ottenere **informazioni riservate**, inducendoti a compiere **azioni** che compromettono la sicurezza delle tue informazioni (es. cliccare su un link per ricevere un codice sconto).

02 Frodi bancarie

I criminali informatici, approfittando dello shopping natalizio, sono soliti **creare delle pagine** web **contraffatte,** come quelle di istituti bancari o di servizi di **pagamento** (es. PayPal), con la finalità di indurti ad effettuare **transazioni** che, invece di arrivare al venditore legittimo, finiscono direttamente nei conti del truffatore.

03 Violazione privacy

Interagire con **allegati** o **link malevoli** che possono nascondersi anche dietro e-mail promozionali o **messaggi** di auguri apparentemente innocui, può favorire **l'installazione di malware**. Questi programmi possono infatti carpire le tue informazioni, monitorare le attività che svolgi sul tuo dispositivo **compromettendo** la tua **privacy**.

Buone pratiche

Se ricevi dei messaggi insoliti che ti inducono a un'interazione immediata, come ad esempio «riscatta il tuo codice promozionale entro due giorni», **non agire d'impulso**: **verifica l'indirizzo** del mittente e ricorda che una offerta troppo bella per essere vera, non lo è!

Prima di effettuare qualsiasi pagamento, assicurati che i siti esterni a cui vieni reindirizzato per concludere le transazioni utilizzino in **protocollo di sicurezza HTTPS.**

In caso di messaggi sospetti, **passa il cursore sul link**: in questo modo potrai visualizzare l'indirizzo reale di reindirizzamento esterno. In caso di indirizzo anomalo, non cliccare, e **segnala** subito l'accaduto all'ufficio competente.

Come difendersi?

Verifica protocollo sicurezza

Durante la navigazione su Internet presta attenzione all'indirizzo web dei siti che stai visitando, specialmente durante le transazioni di **pagamenti digitali**. Accertati che l'indirizzo inizi con «**HTTPS://**». La presenza della lettera «S» dopo «http», indica infatti l'utilizzo del protocollo di comunicazione sicuro, che protegge la trasmissione dei dati attraverso un sistema di crittografia. Questo accorgimento riduce notevolmente il rischio che le informazioni vengano intercettate e/o manipolate.

Attenzione ai codici sconto

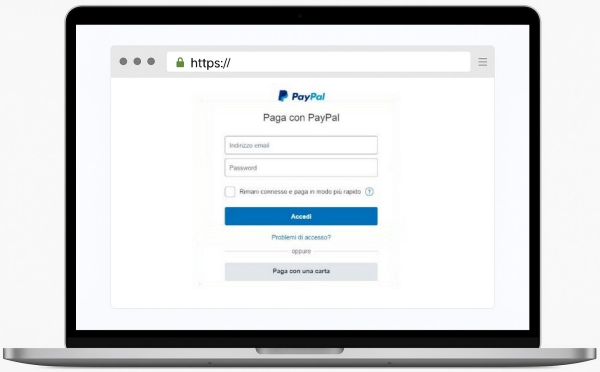
Controlla sempre con attenzione i link, allegati e/o pulsanti, presenti nelle e-mail promozionali o nei messaggi di auguri natalizi, che ti inducono ad interagire con essi. Questi messaggi potrebbero nascondere pericoli come siti malevoli o contenuti dannosi che potrebbero compromettere la sicurezza del tuo dispositivo.

Evitando di interagire con tali contenuti sospetti, ridurrai il rischio di incorrere in attacchi di **phishing** e proteggerai le informazioni sensibili memorizzate sul tuo dispositivo.

Aggiornamenti Periodici

Mantieni sempre aggiornati il sistema operativo, browser e software antivirus sui dispositivi che utilizzi per la navigazione Internet.

In questo modo, non solo migliorerai in modo significativo le **prestazioni** dei tuoi **dispositivi**, ma contribuirai a **ridurre** le **vulnerabilità** di sicurezza (potenziali punti deboli dei sistemi informatici che possono essere sfruttati dagli attaccanti) diminuendo di gran lunga il **rischio** di subire **attacchi informatici con correlate compromissioni.**



Security Trend

La truffa del corriere

Durante il periodo natalizio è stata individuata una **campagna di phishing** che ha sfruttato la popolarità del **corriere GLS** per ingannare gli utenti.

Nello specifico, i criminali informatici hanno inviato **e-mail fraudolente** con l'oggetto "**GLS – Il tuo pacco è in attesa**", facendo leva sull'**aumento delle spedizioni** tipico delle festività. Nel messaggio si invitava il destinatario a **cliccare su un link** per verificare i **dettagli della consegna**, ma il collegamento rimandava a un **sito falso**, graficamente molto simile a quello ufficiale di GLS.

Una volta sul portale contraffatto, gli utenti sono stati indotti a inserire **dati sensibili** e **bancari** che i truffatori miravano ad ottenere al fine di appropriarsi indebitamente di somme di denaro.

Lo schema fraudolento ha avuto particolare successo proprio perché, durante le feste, la probabilità che un utente sia in **attesa** di un **pacco** risulta **notevolmente più alta** rispetto ad altri periodi dell'anno.

Dicembre 2024

Finti Bonus Natalizi

Lo scorso Natale, è stata individuata una **campagna di phishing** nella quale i criminali informatici si sono finti **reparti HR** o **payroll aziendali**.

Nello specifico, le vittime hanno ricevuto **e-mail fraudolente** relative a **presunti bonus di fine anno**, un tema particolarmente **sensibile** durante le festività.

All'interno del messaggio era presente un **allegato** con **codice QR** che, una volta scansionato, rimandava a una **pagina di autenticazione Microsoft falsificata**.

Gli utenti sono stati indotti ad inserire le **credenziali** e i **codici di accesso multifattore**, consegnando inconsapevolmente ai criminali informatici i propri dati di accesso, consentendo così la **compromissione** degli **account aziendali con conseguente** utilizzo illecito delle informazioni sottratte.

Dicembre 2024

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.