MIM
Ministero dell'Istruzione
e del Merito

SICURNAUTI
LA TUA GUIDA NELLA GALASSIA DIGITALE

FESTEGGIA IN SICUREZZA

www.unica.istruzione.gov.it

INDICE DEI CONTENUTI

1 INTRODUZIONE: PERCHÉ LA SICUREZZA DIGITALE È ESSENZIALE DURANTE LE FESTIVITÀ

Durante le festività, l'aumento delle attività online, come l'acquisto di regali, le prenotazioni di viaggi o eventi espone gli utenti a rischi informatici specifici. I criminali digitali sfruttano questa **intensificazione delle transazioni** per mettere in atto truffe, furti di dati e campagne di *phishing*. Le principali minacce si nascondono dietro operazioni apparentemente innocue, come l'acquisto online di regali. Spesso, le transazioni digitali vengono effettuate senza la dovuta cautela, aumentando la possibilità di subire frodi o furti di dati personali.

Anche **messaggi** di auguri ricevuti tramite e-mail, SMS e social media possono contenere ***malware*** progettati per sottrarre dati e monitorare le attività degli utenti. L'emotività legata alle festività può indurre le persone ad **aprire immagini**, allegati e/o ***link*** malevoli, compromettendo la **sicurezza** dei propri dati e delle informazioni.

In Italia, la Polizia Postale registra ogni anno numerose segnalazioni di raggiri digitali, con campagne di ***phishing*** e ***smishing*** che si intensificano nei periodi di sconti e a ridosso del Natale.

Per vivere le festività in modo sicuro e consapevole, è fondamentale adottare comportamenti prudenti e informati. Piccoli gesti quotidiani, come prestare attenzione alle offerte e verificare la sicurezza dei siti, possono prevenire conseguenze gravi, come furti di identità o perdite economiche.

È essenziale che ogni utente adotti **misure** di **sicurezza** informatica, riconoscendo gli **elementi** e le **circostanze** che possono indicare un potenziale **attacco** informatico.

⚠² I PRINCIPALI RISCHI DURANTE I PERIODI FESTIVI

L'aumento degli acquisti online e l'uso più frequente di dispositivi personali offrono ai cybercriminali un'occasione ideale per perseguire i loro scopi.

Questi sono soliti ricorrere a tecniche di **Ingegneria Sociale (o *Social Engineering*)** per manipolare psicologicamente le vittime, con l'obiettivo di ottenere informazioni riservate o indurre a compiere azioni che compromettono la sicurezza dei dati personali come cliccare su un *link* sospetti, ad esempio per ottenere un presunto codice sconto, oppure scaricare allegati malevoli.

Attraverso queste tecniche, gli attaccanti **analizzano i comportamenti online delle vittime** monitorando relazioni, abitudini e attività digitali, al fine di aumentare la probabilità di successo delle loro azioni.

L'Ingegneria Sociale è spesso propedeutica allo svolgimento di campagne di ***Spear Phishing***, una forma di ***phishing* mirata** in cui i messaggi vengono personalizzati sulla base delle informazioni raccolte sulla vittima, come interessi, ricerche recenti o contatti. Questo permette ai criminali di creare contenuti altamente **credibili**, curandone grafica, stile e contesto, in grado di indurre l'utente a visitare siti falsificati, spesso **indistinguibili** da quelli originali.

Il rischio cresce significativamente nei periodi festivi, quando la quantità di notifiche relative ad acquisti, consegne e promozioni aumenta. In questi momenti, il **sovraccarico comunicativo**, **la fretta** e **la diminuzione dell'attenzione** favoriscono le attività degli attaccanti che sfruttano la fiducia degli utenti e l'elevato volume di transazioni online per massimizzare le probabilità di successo delle loro frodi.

Infatti, i cybercriminali intensificano le **truffe** mascherate da offerte o promozioni, sfruttando l'interesse degli utenti per sconti, regali e iniziative commerciali tipiche di questi periodi. Vengono spesso proposte promozioni irrealistiche come *gadget* tecnologici a prezzi eccessivamente ridotti, carte regalo gratuite o *coupon* esclusivi con l'obiettivo di **attirare l'attenzione** di chi è meno attento o attratto da occasioni vantaggiose. Un esempio ricorrente riguarda la diffusione di false promozioni apparentemente riconducibili a marchi noti che rimandano a siti falsificati, appositamente progettati per raccogliere dati di pagamento o credenziali personali.

Queste offerte indirizzano gli utenti verso **pagine di pagamento falsificate**, progettate per sottrarre dati finanziari, oppure verso siti che installano **applicazioni malevole** in grado di compromettere la sicurezza dei dispositivi.

Molti utenti, inoltre, utilizzano i medesimi dispositivi sia per attività personali sia per accedere ai servizi istituzionali. Un dispositivo compromesso può quindi trasformarsi in un **potenziale punto d'ingresso nella rete dell'ente**, facilitando il **furto di credenziali o la diffusione di *malware***.

3 BUONE PRATICHE DI SICUREZZA

In considerazione dei rischi informatici descritti nei paragrafi precedenti, è fondamentale adottare **comportamenti consapevoli e misure di protezione** adeguate. La **prevenzione** è il metodo più efficace per ridurre l'esposizione ai rischi e tutelare le informazioni personali.
Di seguito vengono riportate alcune **buone pratiche di sicurezza**:

Verificare la sicurezza dei siti prima degli acquisti

Durante la navigazione Internet, presta **attenzione all'indirizzo *web*** dei siti che stai visitando, soprattutto durante le transazioni *online*, accertandoti che essi inizino con **«HTTPS://»**. L'impiego di tale protocollo «sicuro» costituisce una forma di garanzia aggiuntiva durante la navigazione: verifica, dunque, che le pagine *web* che visiti riportino la **lettera «S» dopo la dicitura «HTTP»**.

Utilizzare pagamenti sicuri e store ufficiali

Quando effettui acquisti online, utilizza sempre **metodi di pagamento sicuri e affidabili**, evitando bonifici o trasferimenti diretti verso persone che non conosci o che non puoi verificare. Effettua i pagamenti tramite gli ***store* ufficiali** e prediligi **sistemi protetti**, come **carte prepagate o virtuali**, che riducono l'esposizione dei tuoi dati finanziari.
Per una maggiore sicurezza, **controlla con regolarità i movimenti** della tua carta o del tuo conto, così da individuare prontamente eventuali **operazioni sospette o non autorizzate**.

Diffidare delle offerte troppo convenienti

Presta attenzione alle offerte particolarmente **vantaggiose** o alle promozioni che sembrano **poco realistiche**. I criminali informatici possono sfruttare annunci, sconti elevati o messaggi costruiti con tecniche di *social engineering* per indurti a compiere azioni rischiose. Se un prezzo appare eccessivamente conveniente rispetto al valore reale, consideralo come **un possibile tentativo di truffa**.

4 CASI REALI DI INCIDENTI RILEVATI NEI PERIODI FESTIVI

Durante i periodi di grande affluenza di acquisti, come il *Black Friday* e le festività natalizie, aumenta significativamente l'attività dei criminali informatici. Questi periodi generano picchi di registrazioni di domini e campagne online, progettate per ingannare gli utenti sfruttando l'attenzione verso sconti, promozioni e consegne.

Falsi domini e truffe online durante il *Black Friday* 2025

Tra ottobre e i primi giorni di novembre 2025, migliaia di nuovi domini legati al *Black Friday* sono stati registrati, molti dei quali classificati come malevoli. Questi siti erano progettati per richiamare marchi noti, replicandone loghi, grafica e interfacce, e reindirizzavano gli utenti verso pagine apparentemente legittime.

Solo nel mese di ottobre 2025 sono stati identificati **oltre 1.500 nuovi domini** che imitavano *marketplace* reali, con una parte riconosciuta come **minaccia attiva**. Tra i casi documentati, si segnala una frode su un noto nome di calzature sportive, in cui gli attaccanti avevano **replicato fedelmente il sito**, con logo, immagini e prezzi fortemente scontati, inducendo gli utenti a inserire dati personali, credenziali e informazioni delle carte di pagamento. Un altro esempio riguarda una campagna di *phishing* che replicava un grande sito di *e-commerce*, con il dominio costruito per raccogliere credenziali di accesso e informazioni finanziarie degli utenti.
L'utilizzo di domini falsi è una tecnica molto efficace per i criminali informatici perché consente di **aumentare la credibilità dell'inganno**, confondere le vittime e aggirare i sistemi di sicurezza. Creando un sito che sembra autentico, gli attaccanti possono convincere gli utenti a **fornire volontariamente dati sensibili**, massimizzando le possibilità di successo delle truffe e sfruttando eventi ad alto traffico, come il *Black Friday*, per colpire un numero elevato di persone in breve tempo.

SMS FRAUDOLENTI A NATALE

Durante le festività natalizie del 2024, numerosi utenti sono stati colpiti da una campagna di ***smishing***. Nello specifico, gli utenti hanno ricevuto un SMS che annunciava la presunta vincita di un premio in un concorso natalizio di un noto sito di *e-commerce*.
Il messaggio, spesso corredato da nomi o informazioni personali per aumentarne la credibilità, recitava la frase: "Hai partecipato al nostro concorso di Natale e un articolo ti sta aspettando per essere ritirato".

Cliccando sul *link* presente nell'SMS, le vittime venivano reindirizzate a un **sito fraudolento** creato per imitare fedelmente quello legittimo. Qui veniva richiesto di inserire dati personali e bancari, giustificando la richiesta come pagamento di un piccolo contributo per le spese di spedizione.
Gli utenti che fornivano queste informazioni hanno subito **addebiti non autorizzati**, iscrizioni a servizi a pagamento non richiesti e, in alcuni casi, **furto di identità**, con conseguente perdita di accesso ai propri *account*.

Per proteggersi da questo tipo di truffe, è fondamentale non cliccare mai su *link* sospetti ricevuti via SMS, verificare sempre l'autenticità del mittente e inserire dati personali o bancari solo su siti ufficiali e verificati.

Intervento realizzato dal Ministero dell'Istruzione e del Merito e finanziato a valere sul Fondo per la gestione della cybersicurezza nell'ambito della misura 71 e 73 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Agenzia per la Cybersicurezza Nazionale

www.unica.istruzione.gov.it