ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberestafes: un dels perills més grans a l'estiu

TLP: WHITE

JULIOL 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	18/07/2024	22/07/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

Darrerament, s'ha experimentat un increment significatiu de les ciberestafes a l'estiu, i s'han convertit en una de les preocupacions principals tant per a les autoritats, com per als usuaris.

La proliferació d'aquestes amenaces a l'època estival és deguda, a grans trets, al gran volum de viatges i reserves vacacionals que es fan, amb l'augment corresponent de transaccions en línia, i perquè és el moment de l'any en què els usuaris prenen menys precaucions.

Segons dades recentment proporcionades per l'Institut Nacional de Ciberseguretat espanyol (INCIBE), l'estiu de 2023 es van registrar més de 8.000 incidents relacionats amb ciberestafes, un augment del 15 % respecte al mateix període de l'any anterior. Aquest increment és alarmant i evidencia la necessitat d'enfortir les mesures de seguretat cibernètica, tant a nivell individual com institucional.

Les modalitats de ciberestafes són diverses i solen estar relacionades amb reserves de viatges o allotjaments vacacionals fraudulents. Els anuncis de propietats falses o inexistents destinades al lloguer o les campanyes de missatges que simulen ser d'aerolínies, hotels o agències de viatges són algunes de les amenaces principals per als usuaris. De fet, el 2023 més del 40 % de les denúncies de ciberestafes a l'estiu estaven relacionades amb aquesta última tècnica.

Un altre mètode d'estafa que ha guanyat terreny en els darrers anys és la pesca per SMS (l'smishing), una variant de la pesca que fa servir missatges de text SMS per enganyar les víctimes. A la temporada estival de l'any passat, l'INCIBE va informar d'un augment del 20 % en els casos de pesca per SMS, amb un total de 2.500 incidents documentats. Aquest mètode és efectiu per la confiança dels usuaris en l'autenticitat dels missatges rebuts als seus mòbils.

El robatori de dades personals a través d'aplicacions mòbils fraudulentes també s'ha convertit en una preocupació creixent. Amb l'increment de l'ús de telèfons intel·ligents durant les vacances, els ciberdelinqüents desenvolupen aplicacions que simulen que són legítimes, com a eines de navegació o guies turístiques, per extreure informació delicada dels usuaris. El 2023, es van detectar més de 1.200 aplicacions fraudulentes, cosa que representa un augment del 30 % en comparació amb l'any anterior.

I cal no oblidar l'augment tan important de les connexions d'usuaris a xarxes wifi públiques, i no sempre segures, a hotels, aeroports, estacions de tren, o diferents llocs destinats a l'oci, amb els riscos importants que això pot comportar.

Per aquestes raons i davant un panorama de ciberestafes tan prolífic durant l'estiu, en aquest informe es tractaran quines són les causes principals que provoquen el seu augment en aquesta època, quina tipologia de ciberestafes es donen amb una incidència més gran i, com no pot ser d'una altra manera, es facilitaran consells amb els quals ajudar els usuaris a prevenir i protegir-se'n.

3. FACTORS QUE PROVOQUEN L'INCREMENT DE LES CIBERESTAFES

L'augment de les ciberestafes durant la temporada estival a Espanya no és casual ni un fenomen aïllat, sinó que es deu a la confluència de diferents circumstàncies que faciliten les activitats dels ciberdelinqüents.

Tot seguit, es detallen els elements clau que contribueixen a aquest increment.

3.1. Augment de l'ús de dispositius mòbils i xarxes wifi públiques

Els turistes solen dependre dels seus telèfons intel·ligents i tauletes per accedir a informació sobre destinacions, fer reserves i mantenir-se connectats amb amics i familiars.

Aquesta dependència més gran de la tecnologia ofereix als ciberdelinqüents més oportunitats per explotar vulnerabilitats. A més a més, també s'experimenta un increment important de l'ús de xarxes wifi públiques, que es fan servir comunament a cafeteries, hotels i aeroports. Solen ser menys segures i els usuaris en moltes ocasions no són conscients que en connectar-se podrien quedar exposats a diferents accions il·legítimes, com ara el robatori de dades.

3.2. Relaxació de les mesures de precaució dels usuaris

L'època de l'estiu s'associa amb relaxació i descans, cosa que pot dur a prestar una atenció menor a certs detalls, com ara verificar l'autenticitat dels correus electrònics, missatges de text i llocs web, i augmenten la seva vulnerabilitat a tècniques de pesca i pesca per SMS.

3.3. Increment de transaccions en línia

Les compres i les reserves en línia augmenten a l'estiu a causa de les vacances i la planificació de viatges i els ciberdelinqüents fa ja molt temps que aprofiten aquesta tendència i creen llocs web fraudulents que imiten companyies aèries, hotels i agències de viatges legítims.

L'objectiu és enganyar els usuaris i aconseguir que proporcionin informació personal i financera en aquests llocs falsos. Se solen caracteritzar perquè es camuflen darrere de grans ofertes d'últim minut i descomptes molt atractius, que els fan servir com a esquer per atraure les víctimes.

3.4. Exposició a xarxes socials i aplicacions

Molts usuaris ofereixen, sense saber-ho o sense ser-ne conscients, informació molt valuosa als cibercriminals mitjançant l'ús de les xarxes socials. Ús que, a més a més, s'ha comprovat que a l'estiu s'intensifica.

Els estafadors poden explotar tota aquesta informació obtinguda mitjançant Facebook, Instagram o X per crear atacs molt personalitzats i fer-los tan versemblants com sigui possible.

A més a més, també ha de tenir en compte el risc de fer servir aplicacions mòbils fraudulentes, que poden semblar eines útils com a guies de viatge o mapes, i que s'han convertit en un altre vector d'atac en auge. Aquestes aplicacions poden sol·licitar permisos excessius, i obtenen dades personals sense que l'usuari ho sàpiga.

3.5. Una activitat més gran dels ciberdelinqüents

Atesos tots els elements enumerats fins al moment, els ciberdelinqüents intensifiquen la seva activitat durant l'època estival, perquè saben que la taxa d'èxit de les seves accions pot ser més gran.

Fan servir tècniques avançades i sofisticades per evitar ser detectats, i s'adapten ràpidament a les noves mesures de seguretat. L'estacionalitat de la seva activitat reflecteix una estratègia deliberada per explotar els patrons de comportament dels usuaris durant la temporada estival.

3.6. Falta de conscienciació, males pràctiques i bretxa digital

Malgrat els avenços en tecnologia i la prevalença creixent de les ciberestafes, encara hi ha una manca de consciència i educació en ciberseguretat entre molts usuaris.

La manca de coneixement sobre les tècniques de frau més comunes i les millors pràctiques de seguretat fa que els usuaris siguin objectius fàcils. Les campanyes de conscienciació i educació són crucials per mitigar aquest risc, però la implementació i l'abast d'aquestes campanyes sovint són insuficients.

Cal no oblidar que encara hi ha una bretxa digital molt important. Aquesta ha evolucionat i no es caracteritza pel menor accés i ús de persones grans de dispositius mòbils i Internet, sinó per les males pràctiques o coneixements més limitats pel que fa a ciberseguretat.

4. TIPUS DE CIBERESTAFES AMB UNA PREVALENÇA MÉS GRAN

4.1. Pesca i pesca amb SMS

Els correus electrònics i els SMS fraudulents mitjançant els quals els ciberdelinqüents intenten fer-se passar per alguna font o organització de confiança, com ara agències de viatge, hotels, web de reserves o entitats bancàries, estan a l'ordre del dia.

Aprofiten la demanda dels usuaris d'aquesta mena de serveis per llançar campanyes, tant massives com personalitzades, per enganyar usuaris i aconseguir les seves dades personals i, fins i tot, obtenir un rèdit econòmic.

Com ja s'ha comentat anteriorment, les ciberestafes basades en pesca van representar el 40 % de totes les registrades durant l'estiu passat, i les dutes a terme mitjançant el mètode de pesca per SMS, el 20 %.

4.2. Fraus relacionats amb les reserves de viatges

Aquesta mena d'accions s'han vist cada vegada amb més assiduïtat i es poden executar de manera diferent. Per una banda, s'ha vist com els anuncis d'allotjaments vacacionals falsos han incrementat durant cada estiu. Per l'altra, els ciberdelinqüents a vegades es prenen fins i tot la molèstia de replicar un lloc web dedicat a les reserves vacacionals per redirigir allà les seves víctimes i, sense que s'adonin que estan en un lloc fals i il·legítim, robar-los les dades i, fins i tot, desviar les transferències bancàries als seus comptes.

L'Organització de Consumidors i Usuaris (OCU) ha advertit d'un increment significatiu de les denúncies de frau en reserves de viatge durant els mesos estivals. A més a més, el Ministeri de l'Interior i la Policia Nacional espanyols fan campanyes de conscienciació per evitar que els usuaris caiguin en aquests enganys.

4.3. Fraus relacionats amb les compres en línia

La demanda de productes relacionats amb les vacances, com ara roba d'estiu, equips esportius i accessoris de viatge, augmenta a l'estiu. Els ciberdelinqüents creen botigues en línia fraudulentes que ofereixen aquests productes a preus irresistibles.

Tant és així que l'Associació Espanyola de Comerç Electrònic (Adigital) ha compartit que l'estiu ha estat l'època de l'any en què s'ha registrat un augment més gran de les denúncies de frau en compres en línia.

4.4. Ciberestafes relacionades amb connexions wifi públiques

Durant l'estiu, els turistes i estiuejants depenen en gran manera de les xarxes wifi públiques per mantenir-se connectats mentre viatgen. Aquestes xarxes es troben a hotels, aeroports, cafeteries i altres llocs públics. La cerca de connexions de franc i accessibles fa que els usuaris siguin més propensos a connectar-se a xarxes no segures.

Els riscos principals d'aquestes xarxes són la configuració de punts d'accés falsos, per part dels atacants. Mitjançant aquests es pot interceptar el tràfic de qualsevol usuari que hi connecti, i

que es pensa que és una xarxa legítima. El perill és que el cibercriminal aconsegueix interceptar informació personal delicada, claus d'accés o dades relacionades amb targetes bancàries i mètodes de pagament.

4.5. Atacs mitjançant l'ús de diferents tècniques d'enginyeria social

Se sap que en moltes ocasions els ciberestafadors combinen tècniques en línia amb d'altres fora de línia. També s'han registrat denúncies a estafadors que s'han fet passar per empleats d'hotels, empreses de lloguer de cotxes o serveis turístics per aconseguir informació personal o financera de les víctimes o fer ofertes de serveis inexistents.

5. CASOS D'ESTUDI DE CIBERESTAFES RELLEVANTS

5.1. Cas 1: lloguer vacacional fals d'una vil·la de luxe

L'estiu de 2023, un grup de turistes britànics va decidir passar les seves vacances a Espanya i va trobar una oferta atractiva per llogar una vil·la de luxe a la Costa del Sol. La vil·la descrita com una propietat espaiosa amb piscina privada i vistes al mar, estava anunciada en un web conegut d'anuncis classificats. El preu del lloguer era sorprenentment baix en comparació amb altres propietats similars, cosa que va atraure l'atenció dels turistes.

5.1.1. Fases del procés de la ciberestafa

- Anunci atractiu:
    - Els estafadors van publicar un anunci amb fotos atractives de la vil·la, robades d'un lloc web legítim de lloguer de propietats de luxe. La descripció de l'anunci detallava les característiques de la vil·la, incloses diverses habitacions, instal·lacions modernes i una ubicació privilegiada a prop de la platja.
- Comunicació i persuasió:
    - Els turistes van contactar amb el suposat propietari mitjançant el correu electrònic facilitat a l'anunci.
    - L'estafador, fent-se passar pel propietari, va respondre ràpidament i de manera professional, va proporcionar informació addicional i va respondre totes les preguntes dels turistes per generar confiança.
- Sol·licitud de pagament per avançat:
    - Amb l'excusa de l'alta demanda que tenen aquesta mena de residències, l'estafador va indicar a les víctimes que calia fer un pagament per avançat per assegurar la reserva. Els turistes, per assegurar-se el lloguer de la vil·la a un preu tan competitiu, van acordar fer una transferència bancària del 50 % del cost total del lloguer.
- Confirmació falsa:
    - Després de rebre el pagament, l'estafador va enviar una confirmació de la reserva, inclosos els detalls falsos del contracte i un rebut del pagament. Tot semblava legítim i els turistes es van sentir segurs amb la seva elecció.

- Descobriment del frau:
    - En arribar a Espanya, els turistes es van dirigir a l'adreça on suposadament estava la vil·la de luxe i van descobrir que no existia. Van intentar posar-se en contacte amb el suposat propietari, però no va ser possible. En adonar-se que havien estat estafats, van denunciar l'incident a la policia local i a la plataforma web d'anuncis classificats, però no van poder recuperar els diners.

5.2. Cas 2: pesca a reserves de vol mitjançant una companyia aèria falsa

L'any 2022, la protagonista va ser una campanya de pesca que va afectar centenars de viatgers a Espanya i semblava que provenia d'una companyia aèria coneguda, que oferia descomptes exclusius en vols a diverses destinacions populars.

Els estafadors van enviar correus electrònics que incloïen un enllaç per reservar els vols a través d'una pàgina web falsa que imitava la de la companyia aèria real.

5.2.1. Fases del procés de la ciberestafa

- Correu electrònic fraudulent:
    - Els estafadors van enviar correus electrònics mitjançant tècniques de suplantació (spoofing) per tal que semblessin autèntics. Van tenir bona cura del disseny, i fins i tot van fer servir el logotip i altres trets característics del bràndig corporatiu. S'hi oferien descomptes temptadors per fer vols a l'estiu.

- Pàgina web falsa:
    - Els correus electrònics contenien un enllaç que adreçava els usuaris a una pàgina web que imitava perfectament el lloc oficial de la companyia aèria. L'URL era similar a la real, amb diferències mínimes que passaven desapercebudes per a la majoria dels usuaris.

- Recopilació de dades personals i financeres:
    - A la pàgina falsa, els usuaris replicaven el comportament que haguessin dut a terme a qualsevol web legítim, i van introduir les seves dades personals i de pagament per completar la reserva dels vols.

- Confirmació de la falsa reserva:
    - Després de completar el procés de reserva, els usuaris rebien una confirmació falsa per correu electrònic, amb la qual cosa l'estafa encara semblava més legítima. Aquesta acció va permetre guanyar temps als estafadors i aconseguir que fos molt difícil adonar-se'n què estava passant fins que arribés el moment de volar.

- Ús malintencionat de les dades:
    - Les dades són un actiu summament sensible i lucratiu. Els estafadors, després de recopilar-les massivament de moltes víctimes, les van vendre a mercats del web fosc, i a més les van fer servir per fer transaccions fraudulentes amb les targetes de crèdit de les víctimes.
- Descobriment del frau:
    - Les víctimes van descobrir el frau quan van intentar confirmar els seus vols a través del lloc web oficial de la companyia aèria o quan van notar càrrecs no autoritzats a les seves targetes de crèdit.

6. MESURES DE PREVENCIÓ I PROTECCIÓ ENFRONT DE LES CIBERESTAFES

6.1. Consells per a usuaris individuals

- Verificació de l'autenticitat dels anuncis publicats en llocs web i aplicacions d'allotjaments turístics:
    - Fer servir eines de cerca inversa d'imatges per verificar l'autenticitat de les fotos de la propietat.
    - Comprovar l'URL del lloc web per assegurar-se que és l'oficial i no una imitació.
- Ús de plataformes confiables:
    - Reservar a través de plataformes de confiança que ofereixin protecció al client i assegurances en cas de fraus.
    - Llegir ressenyes i opinions d'altres usuaris.
- Comunicació directa i preguntes detallades:
    - Parlar directament amb el propietari a través de la plataforma i fer preguntes específiques sobre la propietat.
    - Sol·licitar un número de contacte i fer una trucada per confirmar detalls.
- Mètodes de pagament segurs:
    - Evitar pagaments per transferència bancària. Fer servir mètodes que ofereixin protecció, com ara targetes de crèdit o serveis de pagament en línia que incloguin assegurances de transacció.
- Sospitar d'ofertes massa bones:
    - Desconfiar d'ofertes que semblin massa bones per ser certes. Fer comparacions amb altres anuncis per assegurar-se que el preu sigui realista.

6.2. Consells per a empreses i organitzacions

- Col·laborar amb les plataformes de reserves en línia:
    - Tenir cura de la cadena de subministrament és fonamental en una estratègia que aposti per una ciberseguretat sòlida. Per això, cal col·laborar amb

plataformes de reserva per millorar els mecanismes de verificació d'anuncis i propietaris.

- També es recomana informar i treballar conjuntament amb les autoritats en casos de frau detectats.

- Fer servir eines de seguretat:
  - Implementar programari de detecció i prevenció d'intrusions (IDS/IPS) i filtres de correu electrònic per identificar i bloquejar missatges de pesca.
  - Fer servir autenticació multifactor (MFA) per protegir els comptes d'usuari.
- Impulsar serveis de monitoratge, alerta prèvia i resposta a incidents:
  - Establir un equip de resposta a incidents de seguretat per gestionar casos de frau i pesca de manera ràpida i efectiva.
  - Monitorar contínuament les xarxes i els sistemes en cerca d'activitats sospitoses.
- Impulsar programes i campanyes de conscienciació internes i adreçades als usuaris:
  - Educar els empleats sobre les tàctiques de pesca i els senyals de frau.
  - Fer simulacions de pesca per millorar la capacitat de detecció dels empleats.
  - Enviar comunicats preventius a usuaris i clients perquè se'n recordin dels riscos de les ciberestafes i com identificar una campanya fraudulenta.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.