ABUSO DNS

DNS ABUSE

Account Locked :unsual excess purchase for alberto AT |12/12/2

AE

American Express <work@secure.net>

Para alberto@soto.net.ar

Seguimiento.

Dear Value Customer,

We've temporarily flagged your card

We are providing this security measures to protect a our customers from an unauthorised use.

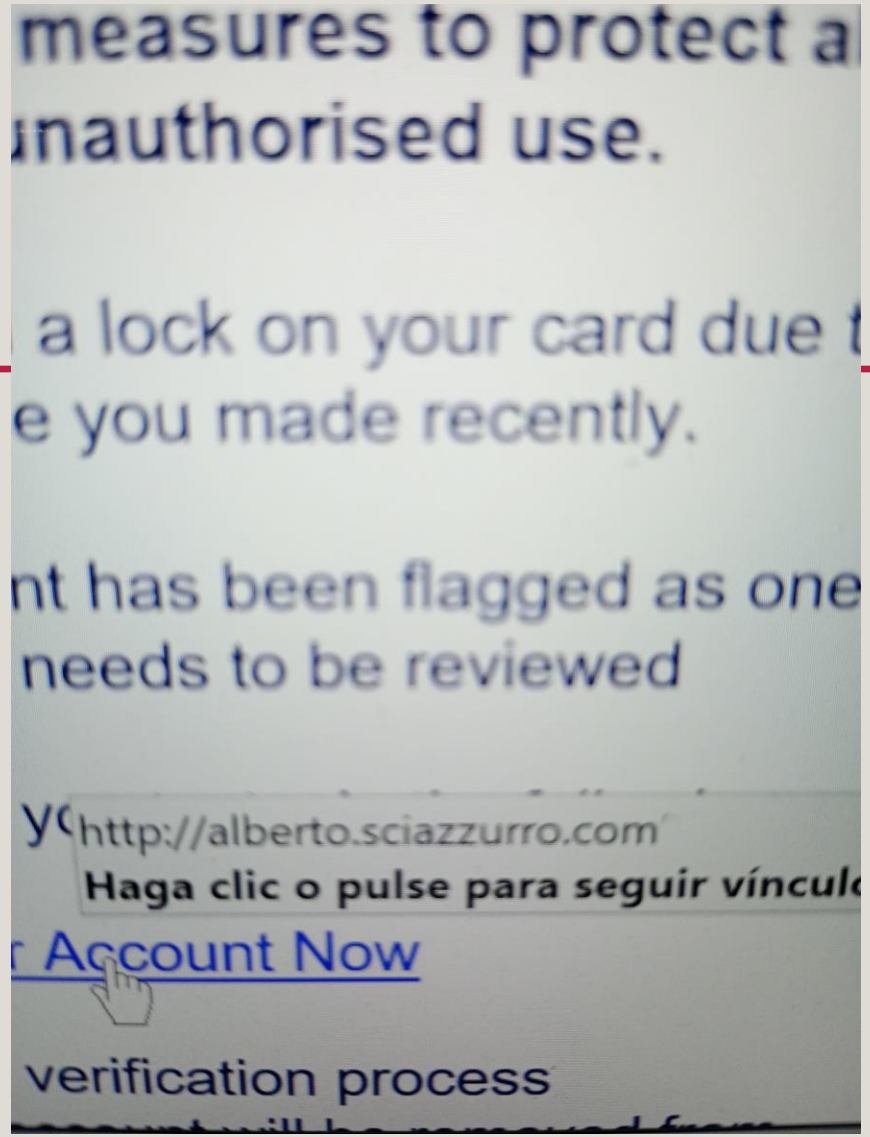
Our fraud department has placed a lock on your card due the unsual excess purchase you made recently.

For security reason, your account has been flagged as or of numerous account that needs to be reviewed

We strongly suggest, that you try to do the following

Review Your Account Now

Complete all verification process



Detectamos un inconveniente de seguridad

BG

Banco Galicia <support@development.w3ondemand.com>

Para alberto@soto.net.ar

5/

Seguimiento.

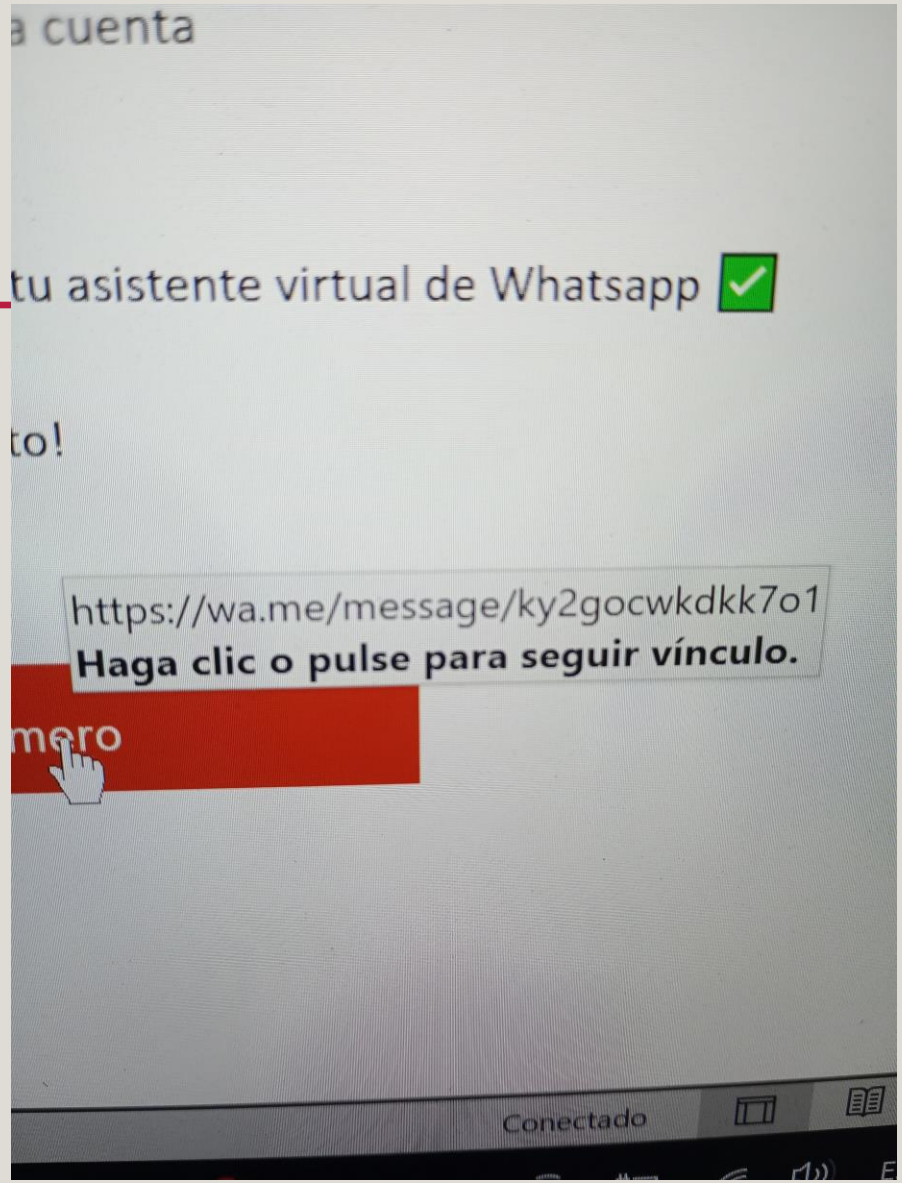
Aviso importante

Nuestro sistema de seguridad contra fraudes determino sus acciones como peligrosas, es necesario que confirme que es el titular de la cuenta
para volver a habilitarla.

Para habilitarla comunicarte con tu asistente virtual de Whatsapp ✅

- Seguí los pasos indicados, ¡y listo!

Certificar Numero



INFORME POLICIAL EMITIDO (ultima advertencia)

PF

POLICIA FEDERAL 915577 <intimaciones91549@notefix.from-wy.c

Para alberto@soto.net.ar

Seguimiento.

BUENOS DIAS SR(A),

De conformidad con el art. 455, § 1 del Código de Procedimiento Civil
se hace presente al **ÍNTIMO**
Su Señoría comparezca, como testigo, en la audiencia que se celebrará
miércoles, 28/11/2023.

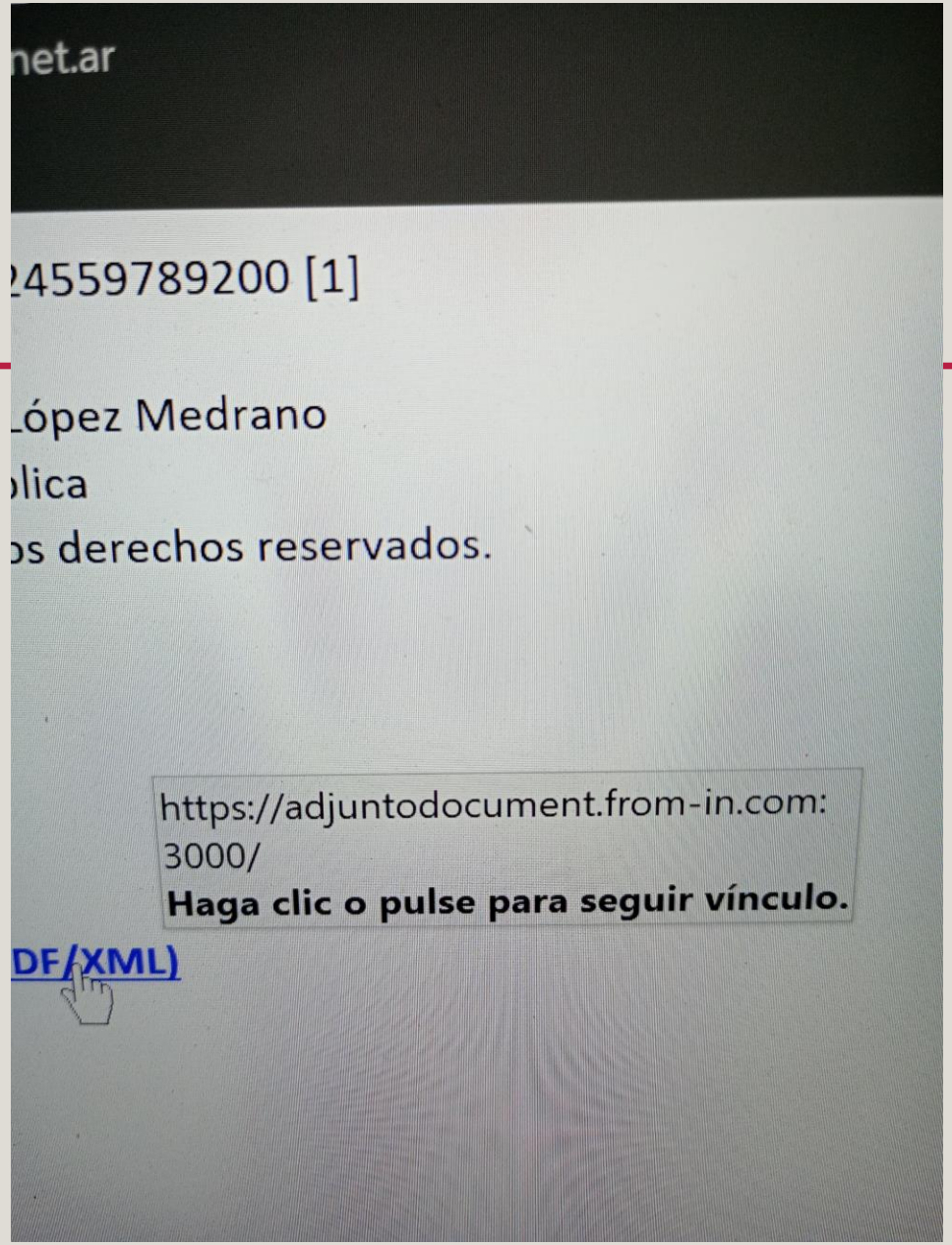
Documento adjunto referente al trámite

CITACIÓN ADJUNTA Nº 50824559789200 [1]

Titular: Lic. Dr. Delio Dante López Medrano
Fiscalia General de la Republica
Copyright (c) 2023, Todos los derechos reservados.

Links:

DESCARGAR CITACIÓN **(PDF/XML)**



Comprobante Electronico - 9851214

DE

Documento Emitido <contacto@accesofinanciero.com>

Para alberto@soto.net.ar

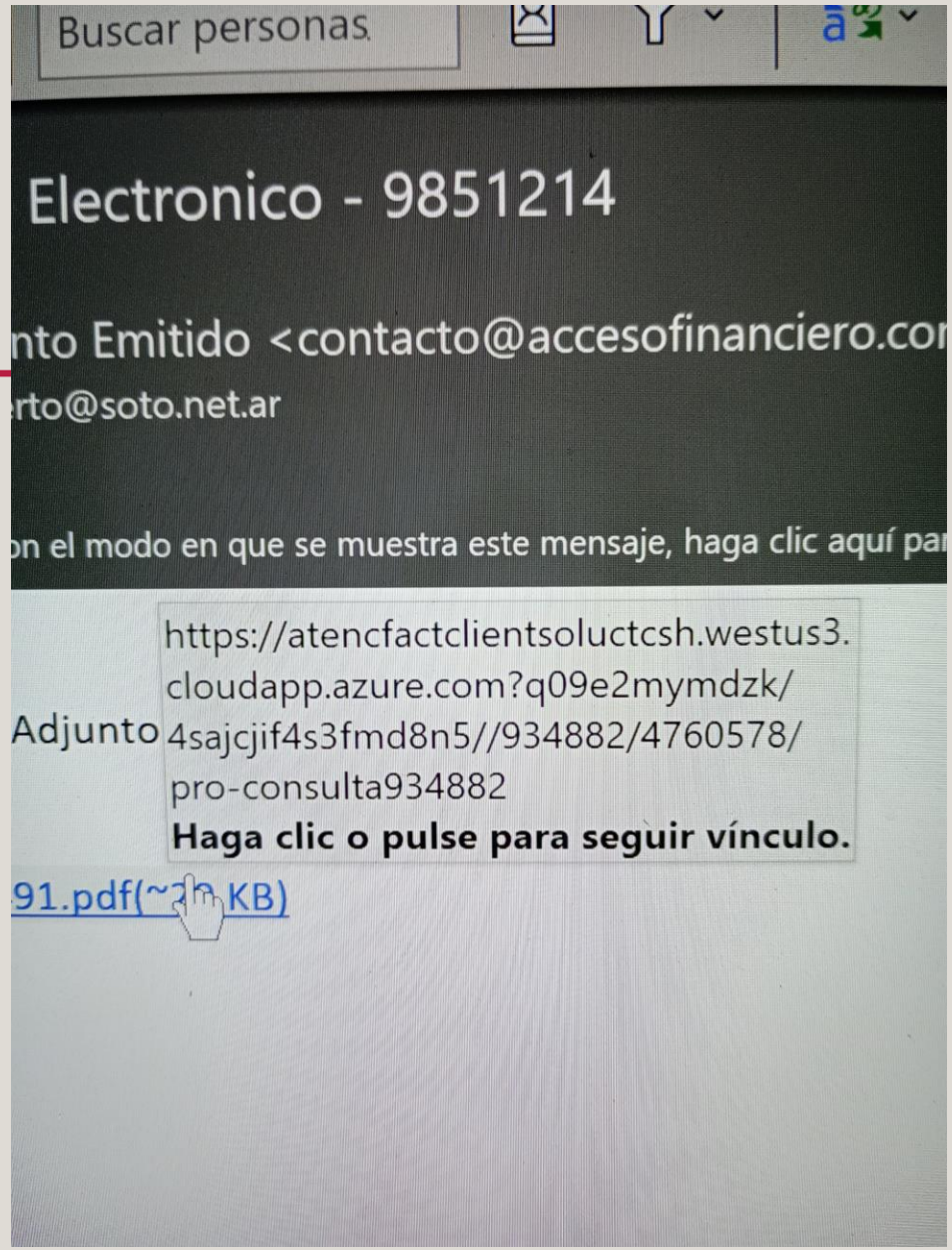
Seguimiento.

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador we

Hola! Como estas? Adjunto Factura de Diciembre.

* FCA0004-00008491.pdf(~20 KB)

Gracias, Saludos.



(((IMPORTANTE))) ACTUALIZACION DEL CORREO WEB - Se requiere c...

S

SOPORTE <soporteproceds2023.cloudns.org@mail.www.com.ar>

Para alberto@soto.net.ar

lunes 11/1

Seguimiento.

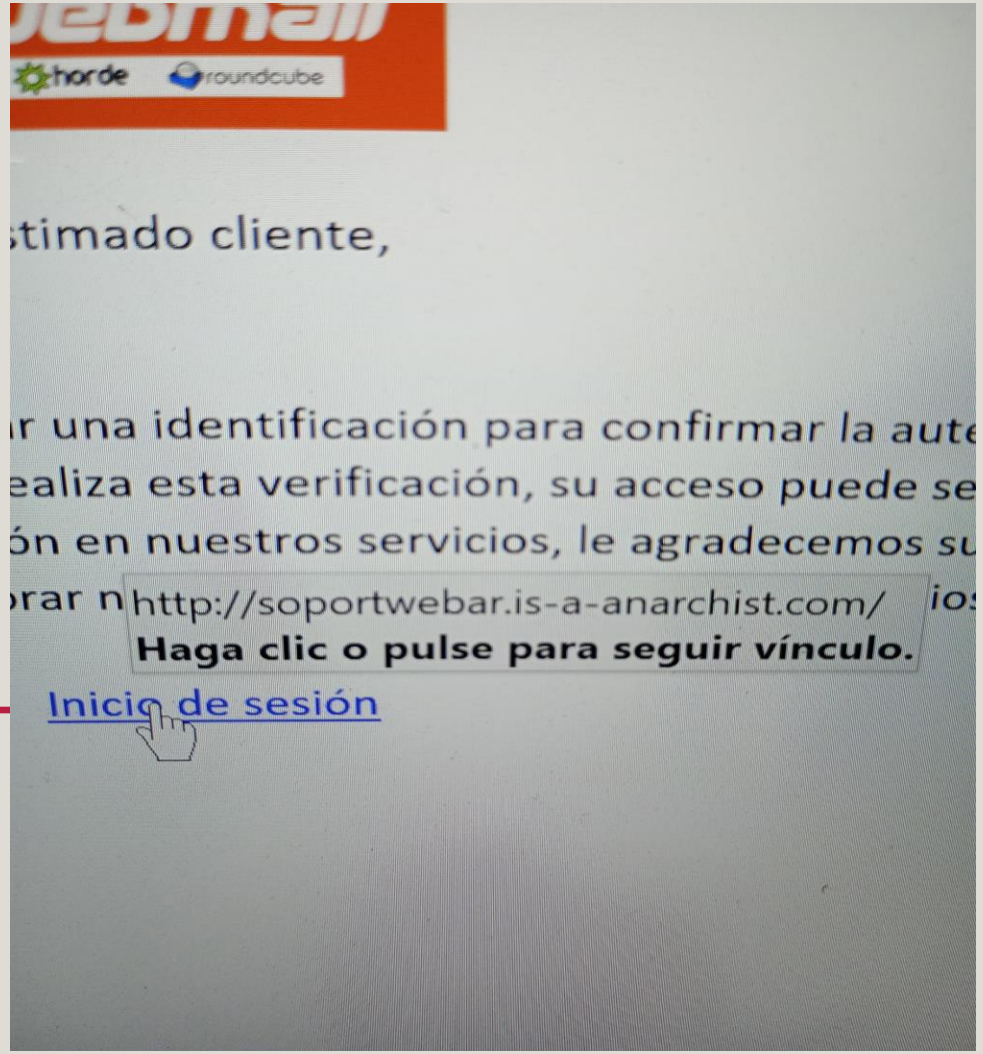
Webmail

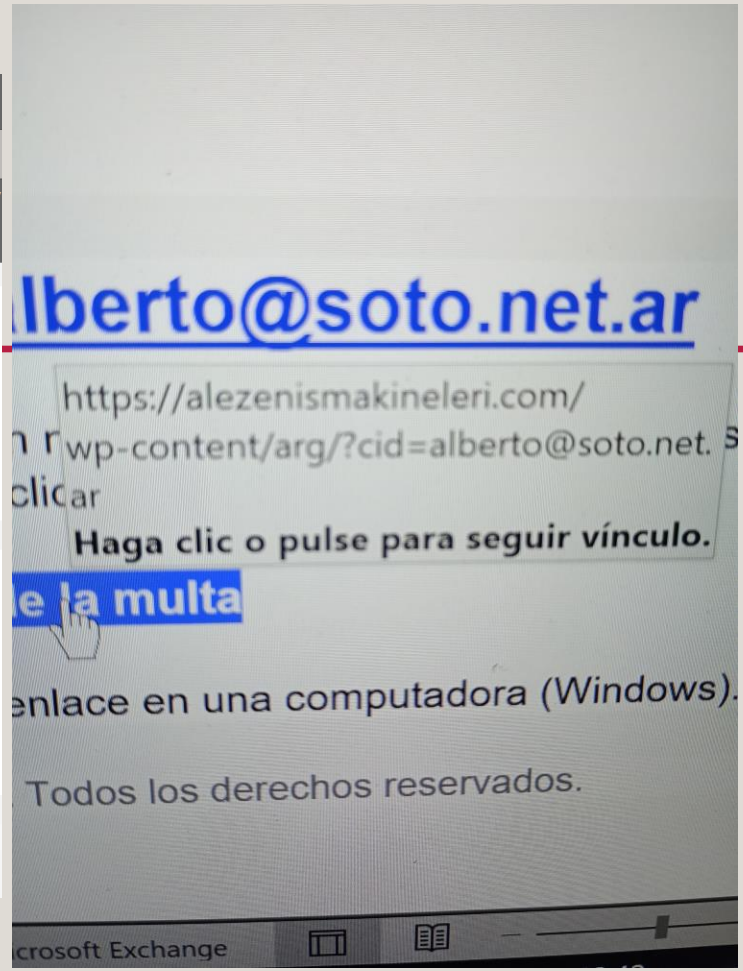
horde roundcube

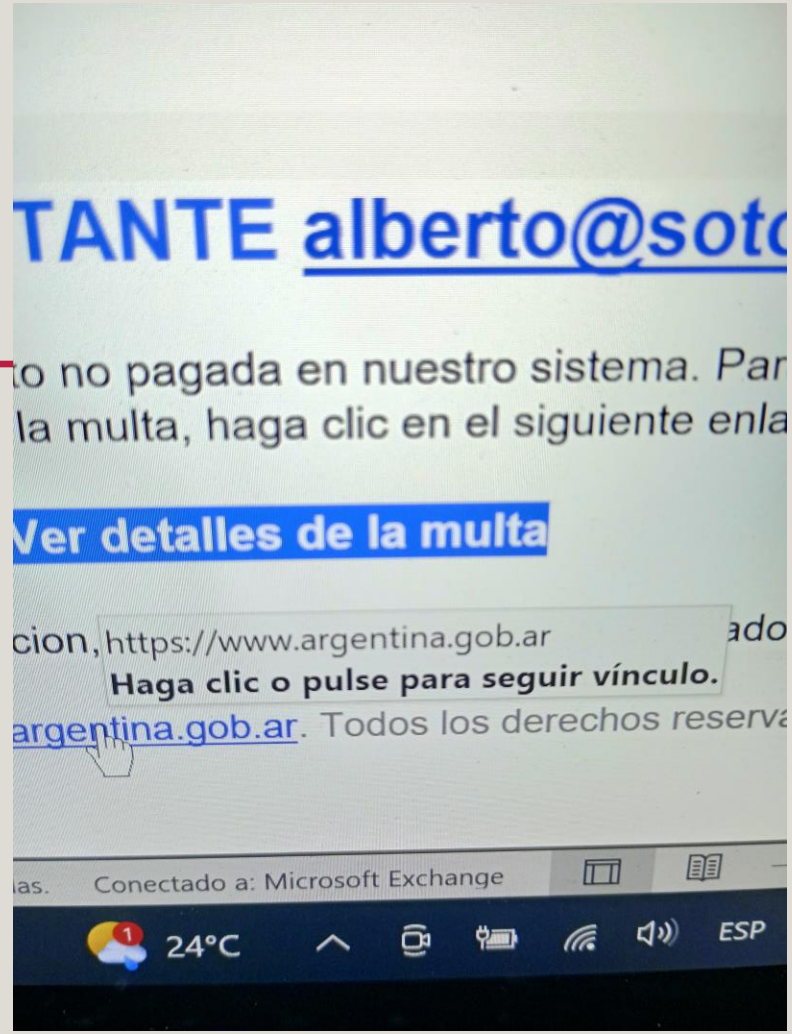
Estimado cliente,

Por razones de seguridad, necesitamos realizar una identificación para confirmar la autenticidad del uso de nuestra plataforma Webmail, si no se realiza esta verificación, su acceso puede ser bloqueado, o incluso provocar la pérdida de su información en nuestros servicios, le agradecemos su colaboración para que siempre podamos mejorar nuestra seguridad con nuestros usuarios.

Inicio de sesión







Subject: Consulta de infracciones SINAI - Atencion Ciudadano alberto@soto.net.ar , le Informamos sobre infracciones Pendientes a su nombre Verifique ahora.

X-PHP-Script: eximiamedical.ro/wp-xml.php for 177.75.23.210

ABUSO DNS – ATAQUES - ATTACKS

Suplantación de DNS/envenenamiento de caché:

DNS Spoofing/Cache Poisoning:

- se introducen datos DNS falsificados en el caché del solucionador de DNS
- **Spoofed DNS data is introduced into the DNS resolver cache**
- provoca que el solucionador devuelva una dirección IP incorrecta para un dominio.
- **causes the resolver to return an incorrect IP address for a domain.**
- En vez de ir al sitio web correcto, desvía el tráfico a un equipo malicioso o a cualquier lugar, quizás a una réplica del sitio original, distribuyendo malware o recopilar información de inicio de sesión.
- **Instead of going to the correct website, it redirects traffic to a malicious computer or somewhere, perhaps a replica of the original site, distributing malware or collecting login information.**

ABUSO DNS – ATAQUES - **ATTACKS**

Túnel de DNS - **DNS tunnel**

- Usa otros protocolos para transmitir consultas y respuestas DNS a través de un túnel.
- **It uses other protocols to transmit DNS queries and responses through a tunnel.**
- Los atacantes pueden utilizar SSH (Secure Shell) ,TCP (Transmission Control Protocol) o HTTP (Hypertext Transfer Protocol) para pasar malware o información robada a consultas DNS, sin que los detecten la mayoría de firewalls.
- **Attackers can use SSH (Secure Shell), TCP (Transmission Control Protocol), or HTTP (Hypertext Transfer Protocol) to pass malware or stolen information to DNS queries, undetected by most firewalls.**

ABUSO DNS – ATAQUES - **ATTACKS**

Secuestro de DNS - **DNS hijacking**

- El atacante redirige las consultas a un servidor de nombres de dominio diferente.
- **The attacker redirects the queries to a different domain name server.**
- Se puede llevar a cabo con malware o con una modificación no autorizada de un servidor DNS.
- **It can be carried out with malware or with an unauthorized modification of a DNS server.**
- Resultado similar a falsificación de DNS, es esencialmente diferente, ya que ataca el registro DNS del sitio web en el servidor de nombres, en vez del caché de un solucionador.
- **Similar to DNS spoofing, it is essentially different in that it attacks the website's DNS record on the name server, rather than a resolver's cache.**

ABUSO DNS – ATAQUES - **ATTACKS**

- Ataque NXDOMAIN: inundación de DNS. Un atacante inunda un servidor DNS con solicitudes de registros que no existen, para causar una denegación de servicio.
- **NXDOMAIN attack: DNS flooding. An attacker floods a DNS server with requests for records that do not exist, to cause a denial of service.**

ABUSO DNS – ATAQUES - **ATTACKS**

- Ataque de dominio fantasma: similar al NXDOMAIN. Se configura una serie de DNSs "fantasmas" que, o bien responden a las solicitudes muy despacio o no responden en absoluto. Después, el solucionador recibe avalancha de solicitudes a estos dominios y inmoviliza esperando respuestas. Consecuencia: rendimiento ralentizado y denegación de servicio.
- **Phantom Domain Attack: Similar to NXDOMAIN. A series of "ghost" DNSs are configured that either respond to requests very slowly or do not respond at all. The resolver then receives a flood of requests to these domains and freezes waiting for responses. Consequence: slowed performance and denial of service.**

ABUSO DNS – ATAQUES – **ATTACKS**

- Ataque de subdominio aleatorio
- **Random subdomain attack**

- Ataque de bloqueo de dominio
- **Domain lock attack**

- Ataque CPE (Common Platform Enumeration) basado en red de robots (botnet)
- **CPE (Common Platform Enumeration) attack based on botnet**

ABUSO DNS- ATAQUES MAS COMUNES - **MOST COMMON ATTACKS**

- Typosquatting: registro de nombres de dominios parecidos a dominios importantes , esperando la equivocación del usuario
- **Typosquatting: registering domain names similar to important domains, waiting for the user to make a mistake**

- Phising: vimos varios ejemplos. Envía enlaces o archivos maliciosos
- **Phishing: we saw several examples. Send malicious links or files**

- Ciberocupación: Registro de dominios para luego abusar en la reventa o utilizarlos como plataforma para cometer ilícitos.
- **Cybersquatting: Registration of domains to then abuse in resale or use them as a platform to commit crimes.**

ABUSO DNS – TECNICAS DE DETECCION E IDENTIFICACION – **DETECTION AND IDENTIFICATION TECHNIQUES**

- Análisis forense de DNS
- **DNS forensics**
- Integración de inteligencia sobre amenazas
- **Threat Intelligence Integration**
- Análisis del comportamiento de la actividad de los dominios
- **Analysis of domain activity behavior**
- Actividad en rangos de direcciones IP propiedad del dominio
- **Activity on domain-owned IP address ranges**

ABUSO DNS – TECNICAS DE DETECCION E IDENTIFICACION – **DETECTION AND IDENTIFICATION TECHNIQUES**

- Seguimiento y análisis de datos WHOIS
- **WHOIS data tracking and analysis**

- Calificación de la reputación de los dominios basada en el aprendizaje automático (soportes SVM, máquinas de soporte de vectores; redes neuronales artificiales)
- **Domain reputation scoring based on machine learning (supports SVM, support vector machines; artificial neural networks)**

ABUSO DNS – CONCLUSIONES - CONCLUSIONS

- El abuso de DNS es un delito
- **DNS abuse is a crime**
- Crece día a día
- **Grows day by day**
- El abuso de dominio se produce cuando un nombre de dominio se utiliza para un fin ilegal o un fin que no es coherente con el uso previsto del nombre de dominio. El propietario normalmente no tiene intención o conocimiento de dicho uso.
- **Domain abuse occurs when a domain name is used for an illegal purpose or a purpose that is inconsistent with the intended use of the domain name. The owner usually has no intention or knowledge of such use**

ABUSO DNS – CONCLUSIONES - CONCLUSIONS

- Debemos tomar conciencia de tres cosas:
  - Que el mayor peligro del Abuso de DNS lo sufre el usuario final, por su desconocimiento técnico.
  - **That the greatest danger of DNS Abuse is suffered by the end user, due to their lack of technical knowledge.**
  - Que como ALSs tenemos la obligación de tomar conocimiento y alertar al usuario final.
  - **That as ALSs we have the obligation to be aware and alert the end user.**
  - Que como ALSs tenemos la obligación de colaborar localmente con la difusión e implementación de DNSSEC.
  - **That as ALSs we have the obligation to collaborate locally with the dissemination and implementation of DNSSEC**

ABUSO DNS – CONCLUSIONES - CONCLUSIONS

ICANN desarrolló el Sistema de Notificación de Actividades de Abuso de Dominios (DAAR) para identificar y rastrear varios tipos de abuso de dominio. Reconocen algunos tipos principales de amenazas a la seguridad en su sistema:

ICANN developed the Domain Abuse Activity Reporting System (DAAR) to identify and track various types of domain abuse. They recognize some main types of security threats on your system:

Spam SEO - Uso de un dominio para manipular el posicionamiento en los motores de búsqueda mediante la creación de páginas de baja calidad que enlazan a otros sitios web.

SEO Spam – Using a domain to manipulate search engine rankings by creating low-quality pages that link to other websites.

ABUSO DNS – DNS ABUSE

THANK YOU SO MUCH

MUCHAS GRACIAS