Ciberseguridad en el FSR

Nuestra Responsabilidad como Empleados

Concientización sobre ciberseguridad

Fideicomiso de Retiro UPR

Primera Parte: Política

JUNTA de Retiro UPR

FIDEICOMISO Sistema de Retiro UPR

Certificación Núm. 16 (2025-2026)

Política de Ciberseguridad

Protegiendo el futuro del Fideicomiso del Sistema de Retiro UPR

Nuestro Propósito Fundamental

En un entorno digital complejo y con amenazas persistentes, la seguridad no es solo una función tecnológica; es un deber fiduciario. El objetivo primordial de esta política es salvaguardar nuestro activo más valioso: **la confianza y el futuro de nuestros miembros**.

Lo que Protegemos

Datos de Participantes y Jubilados(as)

Información de Empleados y Fiduciarios

Infraestructura Tecnológica y Operaciones Críticas

Alcance Sin Excepciones

Esta política aplica a todos los activos de información, independientemente de su ubicación física o de quién los opere.

Los Tres Pilares de Nuestra Seguridad

Confidencialidad: Proteger la información sensible para que no sea divulgada a personas o entidades no autorizadas.

Integridad: Asegurar que la información no sea modificada o destruida sin autorización. Mantenemos su exactitud.

Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a los sistemas en el momento que lo necesiten.

Respaldados por una gestión de riesgos proactiva, cumplimiento legal estricto y mejora continua.

Reglas de Oro del Acceso Operativo

Necesidad de Saber (Need to Know)

- **El Principio:** Tienes acceso únicamente a la información que necesitas para cumplir con tus responsabilidades laborales. Nada más.
- **La Práctica:** Si una información no es vital para tu tarea actual, no debes acceder a ella, aunque el sistema te lo permita.

Menor Privilegio (Least Privilege)

- **El Principio:** Cada usuario o sistema cuenta con los permisos mínimos necesarios para realizar sus funciones.
- **La Práctica:** No operamos con “llaves maestras”. Los privilegios se otorgan a la medida de tu rol para minimizar riesgos en caso de una brecha.

Arquitectura de Defensa en Capas

Acceso e Identidad: Uso de Autenticación Multifactorial (MFA) para accesos remotos/críticos y Redes Privadas Virtuales (VPN).

Protección de Dispositivos (Endpoints): Antivirus, cifrado de datos y actualizaciones regulares de seguridad.

Seguridad de la Red: Segmentación para limitar movimiento lateral en caso de ataque, monitoreo 24/7.

Protección de Datos: Clasificación, cifrado en reposo y en tránsito, copias de seguridad (backups) regulares.

Un Ecosistema Interdependiente: Responsabilidades

Junta de Retiro / Dirección

- Aprobar y respaldar la política.
- Asegurar los recursos necesarios.
- Revisar periódicamente el estado de la ciberseguridad.

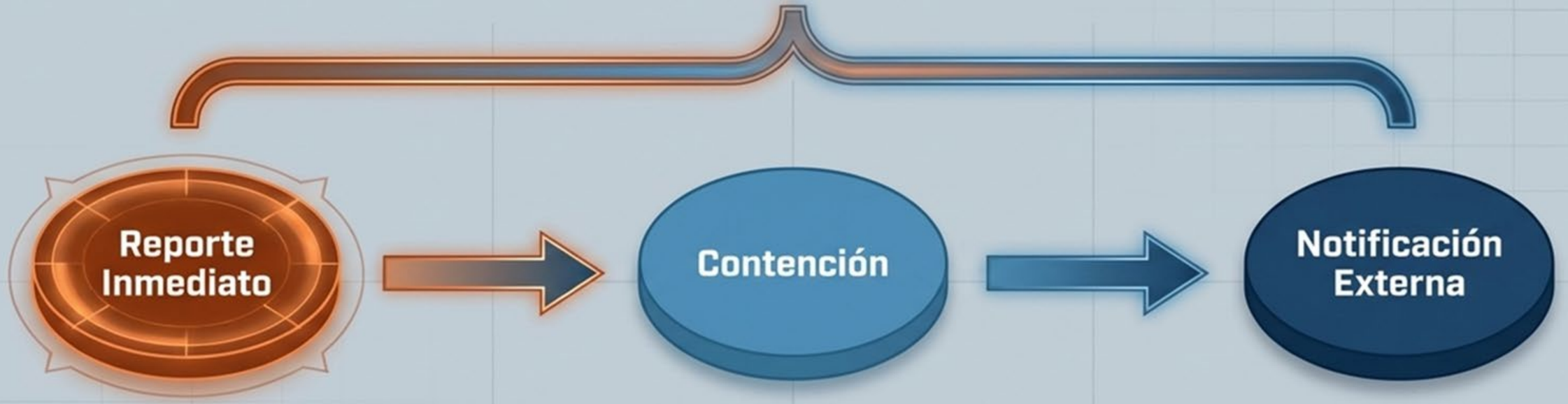
Oficina de Tecnología

- Desarrollar y mantener controles técnicos.
- Supervisar gestión de riesgos y realizar escaneos.
- Dirigir la detección y respuesta a incidentes.

Todos los Usuarios

- Cumplir estrictamente con la política.
- Proteger credenciales y dispositivos (Endpoints).
- Participar en adiestramientos anuales.

Gravedad y Acción: Respuesta a Incidentes



El Usuario: Detección.
Tu responsabilidad es reportar cualquier actividad sospechosa a la OSI de manera inmediata. El reloj comienza a correr.

La OSI: Respuesta.
Contener, erradicar y recuperar los sistemas afectados según el Plan de Respuesta a Incidentes.

El Fideicomiso: Notificación.
En incidentes críticos, la alta gerencia debe notificar a autoridades federales (como el FBI) en un plazo no mayor a 8 horas.

El retraso en el reporte interno imposibilita el cumplimiento federal externo. Tu inacción nos pone en riesgo legal.

Cumplimiento Obligatorio y Consecuencias

El cumplimiento es de carácter obligatorio. El desconocimiento de esta Política no exime de su cumplimiento.

Ciberseguridad en el FSR

Nuestra Responsabilidad como Empleados

Concientización sobre ciberseguridad

Fideicomiso de Retiro UPR

Segunda Parte: Concientización

FIDEICOMISO
DE RETIRO UPR

El eslabón más débil de la cadena de ciberseguridad somos nosotros.

La mayoría de los incidentes comienzan con una decisión humana: un clic, una contraseña débil, una distracción o una confianza indebida.

Por eso, la ciberseguridad moderna no solo protege sistemas; fortalece a las personas, sus hábitos y su criterio.

PERSONAS
Primer punto de entrada.

CONCIENCIA
Reconocer riesgos a tiempo.

HÁBITOS
Pequeñas acciones, gran impacto.

CULTURA
Seguridad como responsabilidad compartida.

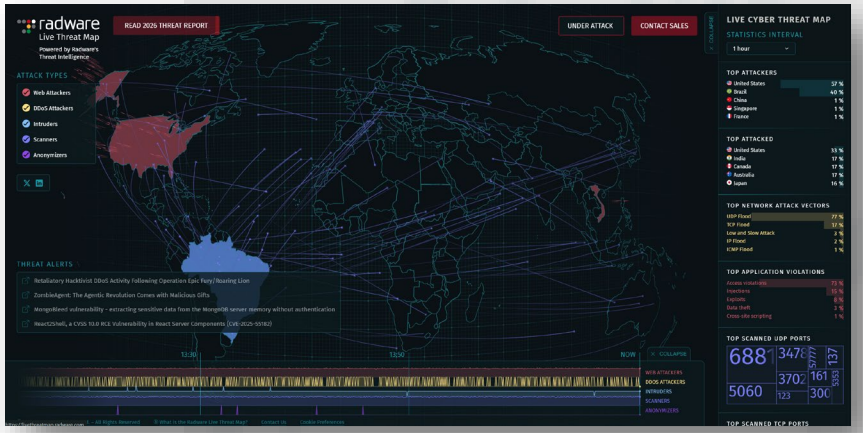
FIDEICOMISO
DE RETIRO UPR

Cuando no estamos atentos...

podemos ser nosotros quienes provoquemos el desastre.

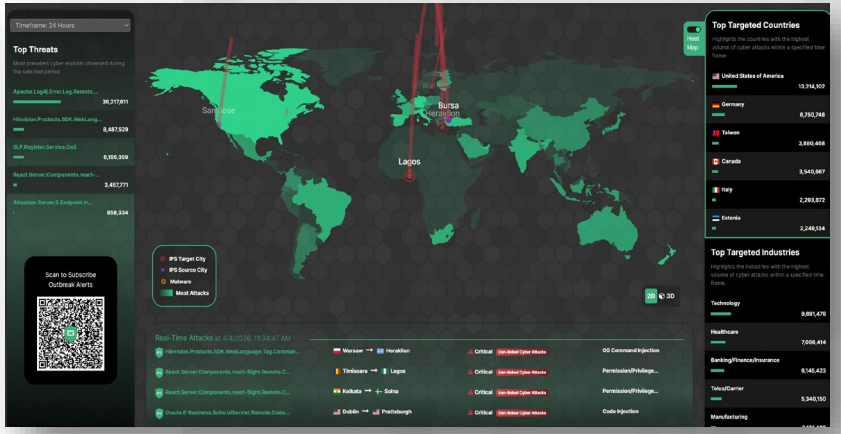
Un clic inocente puede convertirse en un caos.

Estamos en Constante Ataque

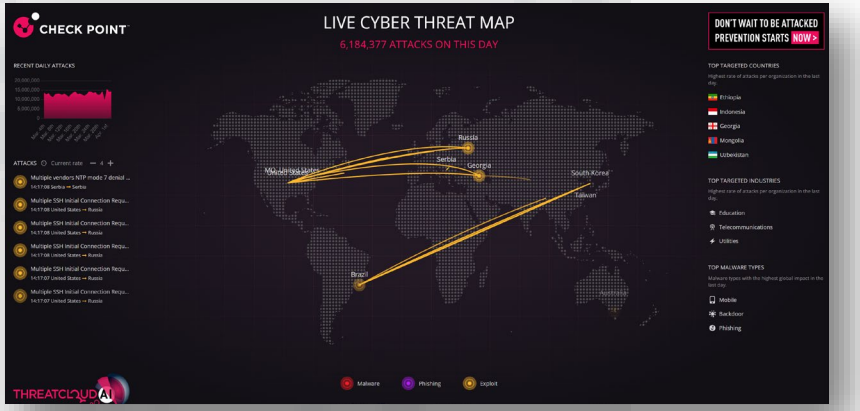


https://livethreatmap.radware.com

https://cybermap.kaspersky.com



https://fortiguard.fortinet.com/threat-map



https://threatmap.checkpoint.com

https://norse-corp.com/map

Ejercicios

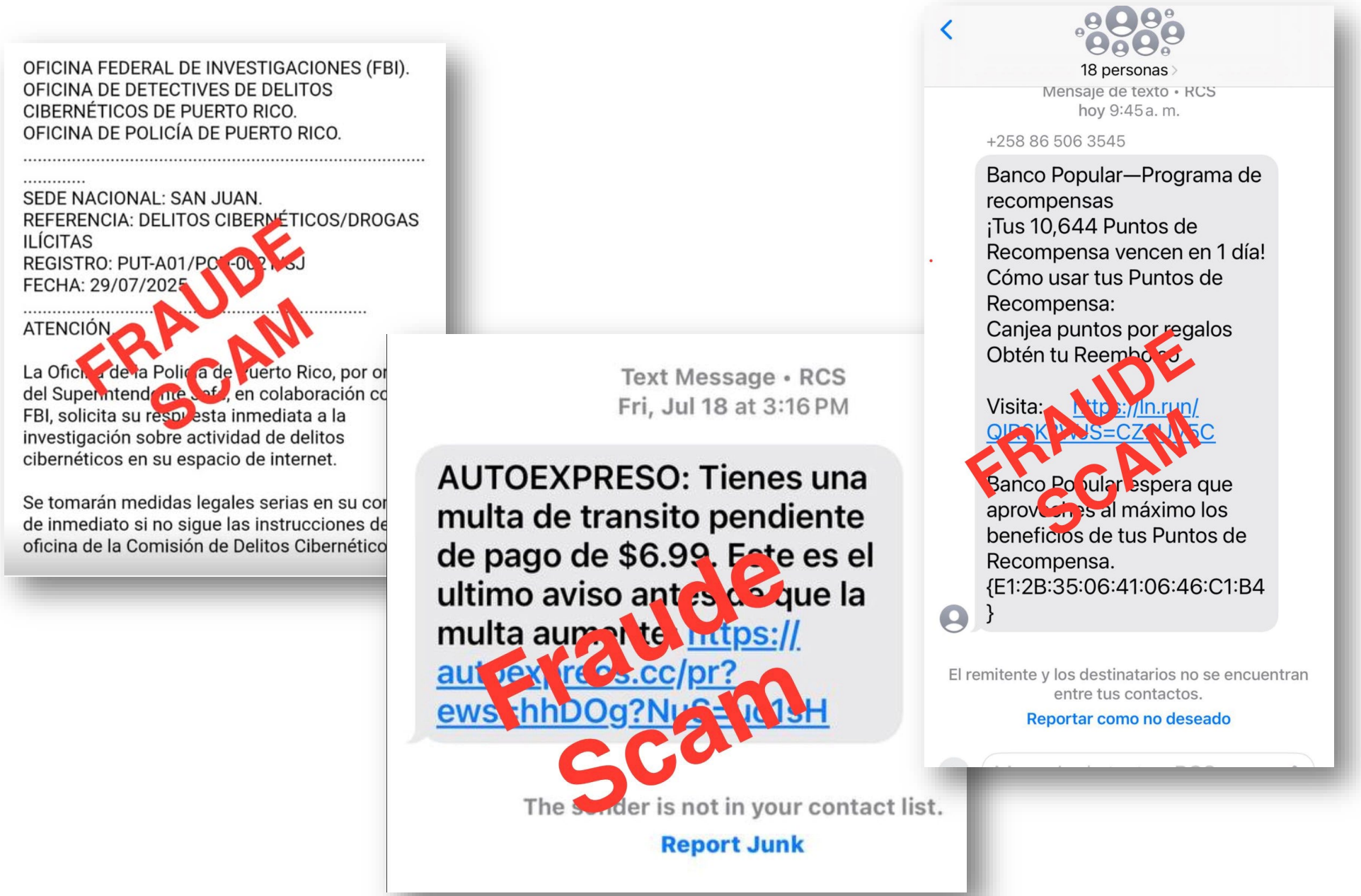
https://mysignins.microsoft.com

https://haveibeenpwned.com

https://www.malwarebytes.com/digital-footprint-app

https://pentester.com

https://databreach.com


OFICINA FEDERAL DE INVESTIGACIONES (FBI).
OFICINA DE DETECTIVES DE DELITOS CIBERNÉTICOS DE PUERTO RICO.
OFICINA DE POLICÍA DE PUERTO RICO.
SEDE NACIONAL: SAN JUAN.
REFERENCIA: DELITOS CIBERNÉTICOS/DROGAS ILÍCITAS
FECHA: 29/07/2025
ATENCIÓN
FRAUDE SCAM
Text Message • RCS
Fri, Jul 18 at 3:16 PM
AUTOEXPRESO: Tienes una multa de transito pendiente de pago de $6.99. Este es el ultimo aviso antes de que la multa aumente
Fraude Scam
Report Junk
18 personas
Mensaje de texto • RCS
hoy 9:45 a. m.
+258 86 506 3545
Banco Popular—Programa de recompensas
¡Tus 10,644 Puntos de Recompensa vencen en 1 día!
Cómo usar tus Puntos de Recompensa:
Canjea puntos por regalos
Visita:
Banco Popular espera que aproveches al máximo los beneficios de tus Puntos de Recompensa.
{E1:2B:35:06:41:06:46:C1:B4}
FRAUDE SCAM
El remitente y los destinatarios no se encuentran entre tus contactos.
Reportar como no deseado

Nadie es Inmune

Landmark Admin
(800,000 personas)

Números de Seguro Social, información médica y pólizas de seguro.

23andMe
(7 Millones)

Historiales genéticos. árboles genealógicos (hackeado mediante contraseñas antiguas).

Change Healthcare
(100 Millones)

El mayor hackeo de datos de pacientes en la historia de EE. UU.

National Public Data
(2.9 Billones)

Grupo USDoD / Fenice filtró 277 gigabytes de nombres, historiales de direcciones de tres décadas y SSNs.

usatoday.com/story/tech/2024/08/17/social-security-hack...

USA TODAY

BREAKING NEWS: George Santos pleads guilty to two counts in federal c

U.S. Elections Sports Entertainment Life Money [Tech] Travel Opinion

TECH

Data Breach Add Topic +

National Public Data confirms massive data breach included Social Security numbers

Social Security numbers, names, addresses, email addresses and phone numbers were in the 2.9 billion records within a data breach. Security firm Pentester.com tool tells you if yo

Mike Snide
USA TODAY

Published 5:30 p.m. ET Aug

securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citi

SecurityIntelligence

National Public Data breach publishes private data of 2.9B US citizens

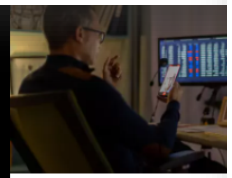
Light Dark

August 19, 2024
By Jennifer Gregory
3 min read

News

Billions of people's data was published on the dark web around April 8, 2024 — from a single breach of National Public Data. However, many of the victims are still unaware of their exposure because they have yet to receive a notification or statement from the company.

Recently, one of the victims filed a class action lawsuit after learning that their data was breached when they received a notification from an identity theft protection service provider. What will this mean for people whose data was unknowingly sold on the dark web?



DATA PROTECTION | August 13, 2024

Cost of a data breach 2
Financial industry

3 min read - According to the IBM Co
Breach 2024 report, the average glo
has reached $4.88 million — a signif
over last year's $4.45 million and th

DATA PROTECTION | August 6, 2024

CNBC

Search quotes, news & videos WATCHLIST | SIGN IN CREATE FRE

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO MAKE IT SELECT USA • INTL

PERSONAL FINANCE

2.9 billion people may have had Social Security numbers, other financial data compromised. What it means for you

PUBLISHED THU, AUG 15 2024-3:19 PM EDT | UPDATED THU, AUG 15 2024-7:40 PM EDT

Lorie Konish

SHARE

KEY POINTS

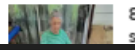
- About 2.9 billion people may have had their personal financial data compromised, a lawsuit alleges.
- "It's not a matter of if, it's a matter of when" you may be personally affected by a breach, one expert says.
- Experts say there's one best step to take to protect your personal data.

TV

Closing Bell: Overtime WATCH LIVE

UP NEXT | Fast Money 05:00 pm ET Listen

TRENDING NOW



85-year-old mom who co-signed daughter's

Aug 15, 2024

2.9 billion records, including Social Security numbers, stolen in data hack

- El grupo de piratas informáticos USDoD afirmó el robo de **registros personales de 2.900 millones de personas** de National Public Data
- **National Public Data** es una compañía de verificación de antecedentes con sede en Florida operada por Jerico Pictures, Inc
- 277,1 gigabytes de datos, e incluye **nombres, historiales de direcciones, familiares y números de Seguro Social** que se remontan al menos a tres décadas.
- USDoW afirma estar vendiendo los 2.9 mil millones de registros para ciudadanos de los EE. UU., el Reino Unido y Canadá
- Un hacker conocido como "Fenice" **filtró la versión más completa de los datos de forma gratuita en un foro en agosto 2024.**

https://npd.pentester.com

MoneyWatch

16 billion login credentials from Google and other sites leaked online, report says

June 20, 2025 / 3:05 PM EDT / CBS/AP

Sixteen billion login credentials have been leaked and compiled into datasets online, giving criminals "unprecedented access" to accounts consumers use each day, according to researchers at cybersecurity outlet Cybernews.

According to a report published this week, Cybernews researchers have recently discovered 30 exposed datasets that each contain a vast amount of login information — amounting to a total of 16 billion compromised credentials. That includes user passwords for a range of popular platforms including Google, Facebook and Apple.

Because 16 billion is roughly double the amount of people on Earth today, the number signals that impacted consumers may have had credentials for more than one account leaked. Cybernews notes that there are most certainly duplicates in the data and so "it's impossible to tell how many people or accounts were actually exposed."

Related News

Iran Using Ceasefire To Dig Out Weapons It Had Hidden Underground: Report

Iran Delivers New Proposal To Pakistan For US Peace Talks: Report

60-Day Deadline Hours Away, Team Trump Denies Being At War With Iran

Trending News

1 JPMorgan Executive Accused Of Sexually Abusing 'Brown Boy Indian': Report

2 Poison, Not Watermelon, May Have Killed 4 Of Mumbai Family, Say Sources

3 "Saw My Mother Drown": Jabalpur Boat Accident Survivor Recounts Horror

4 35 US Lawmakers Just Moved A Bill That Could Wreck Indian Techies' Careers

5 Mother, Son's Bodies Found Holding Each Other In Cruise Boat Tragedy

Home Addresses Of Over 2,000 US Marines Leaked By Iran-Linked Group: Report

According to The Wall Street Journal, the hackers shared identifying information on Telegram, presenting the leak as evidence of their "surveillance capabilities".

Edited by: Anushree Jonko | World News | Apr 29, 2026 22:33 pm IST

Read Time: 3 mins

Share

Hackers presented leak as evidence of their "surveillance capabilities"

Show Quick Read
Summary is AI-generated, newsroom-reviewed

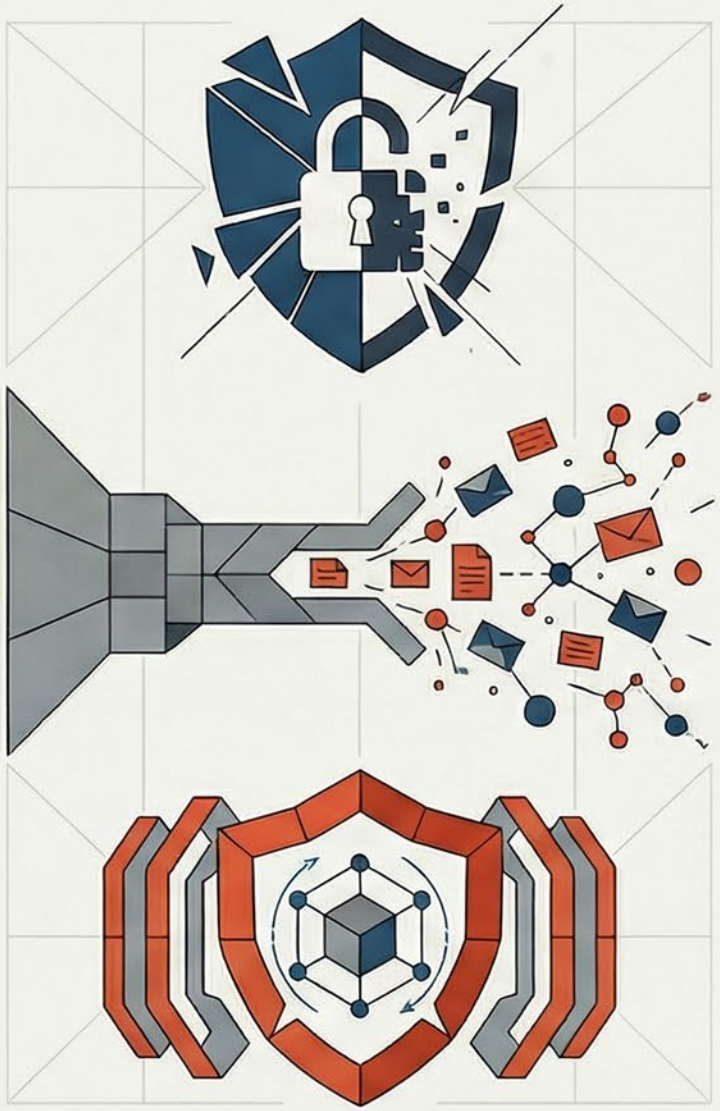
A cyber group known as Handala, believed to have links to Iran, claimed on Tuesday that it had released personal information of US Marines deployed in the Persian Gulf. In a post on its Telegram channel, the group said it had published the names and details of 2,379 personnel.

According to The Wall Street Journal, the hackers shared identifying information on Telegram, presenting the leak as evidence of their "surveillance capabilities".

Iraq-based Shafaq News reported that the US personnel stationed in the region were sent threatening messages on WhatsApp, warning that they were under watch and could be targeted. The group further claimed it had access to deeper layers of data, including family information, home addresses, and even details about daily routines and troop movements. It also signalled that more disclosures could follow.

BLINDAJE DIGITAL

La protección de datos ya no es automática, es una responsabilidad personal activa.



Ante la exposición inminente, la pregunta crítica es

¿Qué hago?

La privacidad total es una ilusión.

Es ingenuo asumir que nuestra información personal está completamente protegida en las plataformas digitales actuales.

Brechas de datos: una realidad inevitable.

Las filtraciones masivas han expuesto la información de millones, vulnerando la seguridad de casi todos los usuarios.

¿Qué hago?

https://www.usa.gov/credit-freeze

El Nuevo Paradigma de la Seguridad: De Dispositivos a Personas

La seguridad digital ha evolucionado de un modelo centrado en la infraestructura física hacia uno centrado en el factor humano.
Este cambio reconoce que el individuo es ahora el punto crítico de protección en el entorno tecnológico actual.

El Enfoque Tradicional

Seguridad de Computadoras

El modelo histórico basado estrictamente en la protección de activos físicos y hardware.

Enfoque en el Objeto

Priorización de perimetros técnicos y dispositivos aislados sobre el comportamiento humano.

El Nuevo Paradigma

Seguridad Centrada en las Personas

La transición hacia el aseguramiento del indivíduo como núcleo de la estrategía.

“Estamos asegurando personas...”

Reconocimiento del factor humano como el eslabón primordial en la seguridad moderna.

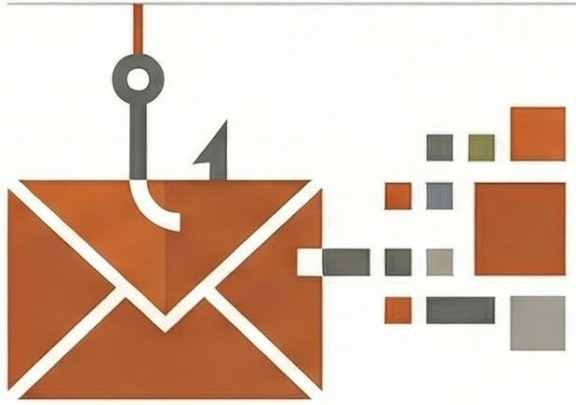
Amenazas de Ciberseguridad: Conceptos Fundamentales

Tácticas de Manipulación psicológica y el uso de software malintencionado

MANIPULACIÓN HUMANA Y ENGAÑO

INGENIERÍA SOCIAL

Técnica de manipular a las personas para que provean accesos y/o información confidencial.



PHISHING

Engaño mediante correos electrónicos para motivar acciones indebidas de la víctima.

SOFTWARE MALICIOSO

MALWARE

Software diseñado para interrumpir, dañar u obtener acceso no autorizado a sistemas.

[redacted]

DM

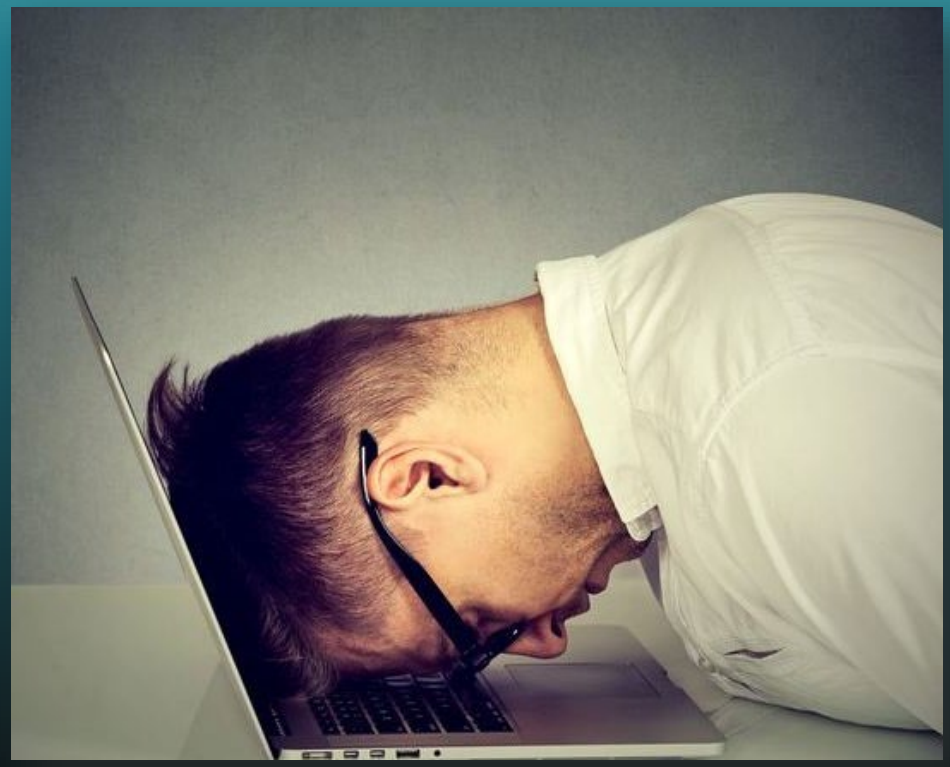
Dr. Miguel Vélez Rubio
officepstmailverbanc@gmail.com

To: You [redacted]

Thursday, November 7, 4:00 PM

Hola, ¿Tienes un momento? Tengo una solicitud que necesito que manejes discretamente. Estoy teniendo una reunión en este momento, no hay llamadas, así que solo responde mi correo electrónico.

Dr. Miguel Vélez Rubio
Rector
Enviado desde mi Correo para Samsung



No se deje engañar…

De: [redacted]@gmail.com>
Enviado: martes, septiembre 24, 2024 4:16 p. m.
Para: [redacted]@upr.edu>
Asunto: Re: Urgente

Necesito que vayas a Walgreens y me ayudes a comprar una tarjeta Apple de 200 $. Lo necesito justo en la reunión. Lo recibirás por correo electrónico, te reembolsaré tan pronto como termine la reunión. Por favor, lo necesito urgentemente.

[redacted]

Catedrática Asociada, Directora
Departamento de Química
Ubicación de la oficina: Q-2
UPR Bayamón

Universidad de Puerto Rico

IMPORTANTE: SE NECESITA VERIFICACIÓN DE CUENTA DE 0FFICE.365

Este sitio web verifica a todos los estudiantes y confirma su correo electrónico @upr.edu para que su cuenta no se cierre.

Proporcione rápidamente los detalles de su correo electrónico @upr.edu y esté listo para mostrar un código cuando nuestros agentes de TI se comuniquen con usted.

Para evitar que su cuenta se cierre en las próximas 48 horas, actúe ahora y solucione este problema.

Lea las instrucciones a continuación y complete el formulario para obtener más ayuda.

Sign in to Google to save your progress. Learn more

* Indicates required question

NOMBRE COMPLETO *

Your answer

INGRESE SU DIRECCIÓN DE CORREO ELECTRÓNICO @upr.edu *

Your answer

*

Contraseña

Your answer

From: [redacted]
Sent: Tuesday, October 8, 2024 7:56:42 AM
Subject: ¡RESPUESTA URGENTE!

¡Felicitaciones! Usted ha sido seleccionado como candidato potencial para un puesto remoto disponible que ofrece $500 por asignación. Para obtener más información sobre las funciones y responsabilidades del puesto

Envíe su:
NOMBRE COMPLETO:
NÚMERO DE TELÉFONO:
DIRECCIÓN DE CORREO ELECTRÓNICO:
A MELOSCUFIELD234@OUTLOOK.COM

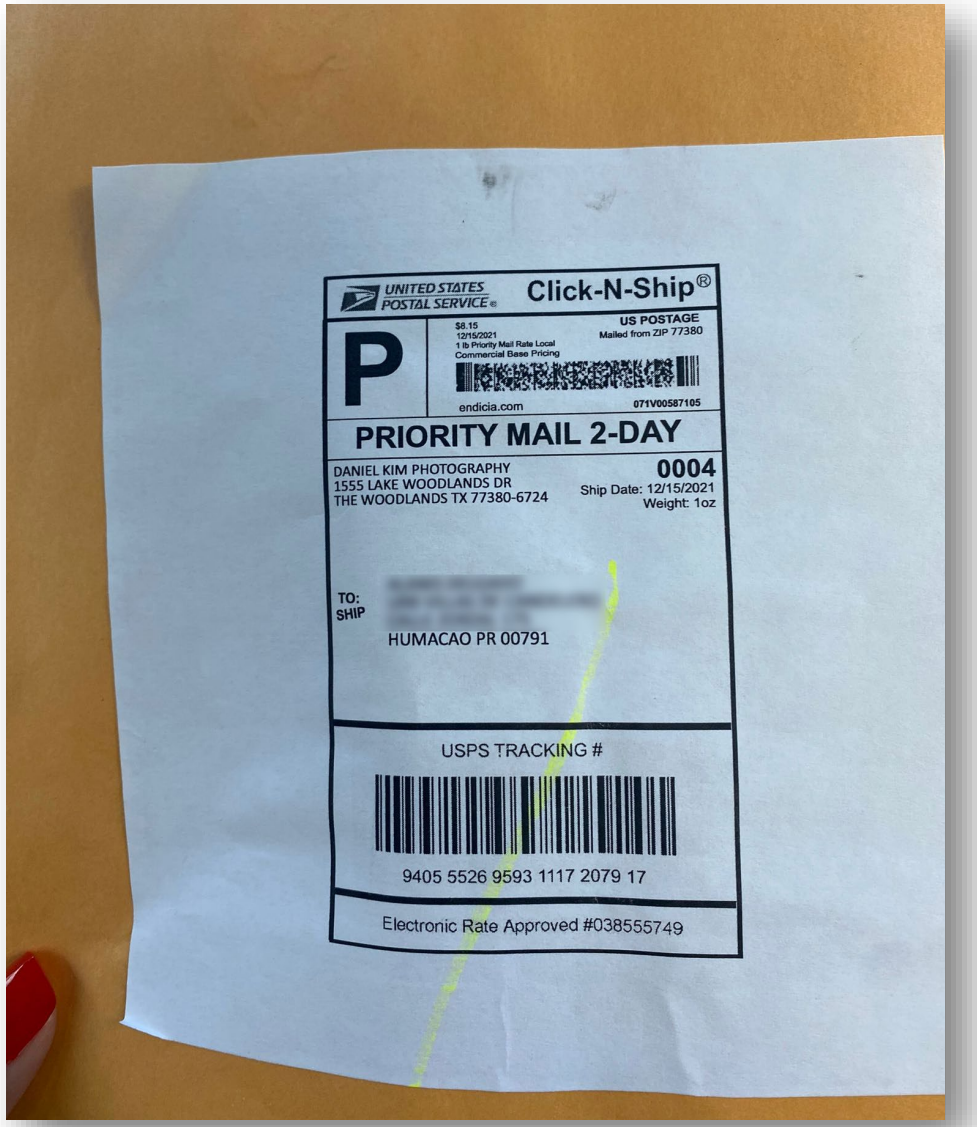
From: [redacted]@upr.edu>
Sent: Wednesday, September 25, 2024 4:24 PM
Subject: willing to work and earn?

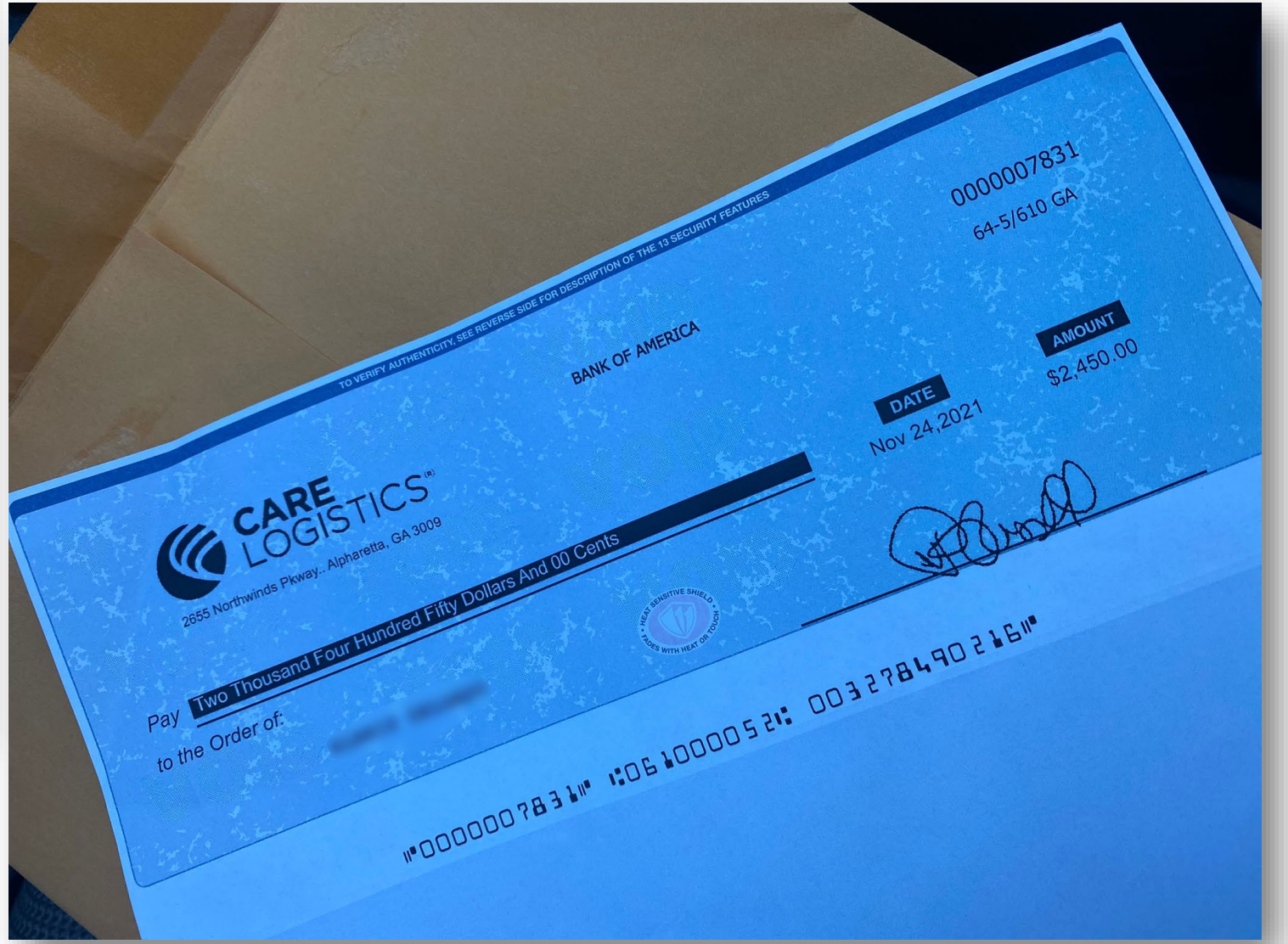
The Office of Job Placement and Student Services is pleased to announce remote internship positions available to students facing financial hardship. These opportunities offer a combination of financial support and valuable research experience.

Interns will work remotely, with flexible schedules accommodating up to seven hours per week. A stipend of $350 per week will be provided. This program is open to all UPR Puerto rico students, regardless of major.

Due to limited positions, applications will be considered on a first-come, first-served basis. Interested students should contact Dr. Juan Medina Lee at [redacted] via text to inquire about eligibility and the application process. Please include your full name, email address, department, and current year of study.

We encourage qualified students to submit their applications promptly.
Sincerely,
Dr. Juan Medina Lee Assistant Professor,
Department of Computer Science Universidad de Puerto Rico,
Puerto Rico


UNITED STATES POSTAL SERVICE
Click-N-Ship®
P
$8.15
12/15/2021
1 lb Priority Mail Rate Local
Commercial Base Pricing
US POSTAGE
Mailed from ZIP 77380
endicia.com
071V00587105
PRIORITY MAIL 2-DAY
DANIEL KIM PHOTOGRAPHY
1555 LAKE WOODLANDS DR
THE WOODLANDS TX 77380-6724
0004
Ship Date: 12/15/2021
Weight: 1oz
TO:
SHIP
HUMACAO PR 00791
USPS TRACKING #
9405 5526 9593 1117 2079 17
Electronic Rate Approved #038555749


TO VERIFY AUTHENTICITY, SEE REVERSE SIDE FOR DESCRIPTION OF THE 13 SECURITY FEATURES
0000007831
64-5/610 GA
BANK OF AMERICA
AMOUNT
$2,450.00
DATE
Nov 24,2021
CARE LOGISTICS®
2655 Northwinds Pkway., Alpharetta, GA 3009
Pay Two Thousand Four Hundred Fifty Dollars And 00 Cents
to the Order of:
HEAT SENSITIVE SHIELD
FADES WITH HEAT OR TOUCH
⑈0000078316⑈ ⑆061000052⑆ 003278490216⑈

Guía de Beneficios y Aumento de Compensación 2026

U

University of Puerto Rico School of Medicine<victor.diaz@upr.edu>

To: USERNAME <victor.diaz@upr.edu>

Sat 4/4/2026 4:06 PM

Revisión de Ajuste de Nómina y Bonificación

Preparado por el Equipo de Recursos Humanos y Nómina

Tiempo: March 31, 2026 06:15:49 PM

Para acceder a la vista completa, por favor escanee el código QR abajo utilizando un dispositivo móvil.

Este mensaje incluye un enlace a un recurso de SharePoint. Por favor, maneje esta información conforme a las prácticas internas estándar.

Dirección de Correo Electrónico: victor.diaz@upr.edu

Fw: University of Puerto Rico School of Medicine Notificación de Aprobación: Revisión Completada el March 31, 2026 06:15:48 PM Summarize this email

VD

Victor Diaz<victor.diaz@upr.edu>

To: Victor E Diaz Rodriguez

Sat 4/4/2026 4:06 PM

Informe de Ajuste de Pago d...
265 KB

Víctor Diaz

From: Victor Diaz <victor.diaz@upr.edu>
Sent: Tuesday, March 31, 2026 2:30:24 PM
To: Pablo Rebollo-Sosa <pablo.rebollo@upr.edu>; Jose R Pabon Pagan <jose.pabon2@upr.edu>
Subject: Fw: University of Puerto Rico School of Medicine Notificación de Aprobación: Revisión Completada el March 31, 2026 06:15:48 PM

Phishing

Víctor Diaz

From: University of Puerto Rico School of Medicine <info@stalenramendeprez.be>
Sent: Tuesday, March 31, 2026 2:15:53 PM
To: Victor Diaz <victor.diaz@upr.edu>
Subject: University of Puerto Rico School of Medicine Notificación de Aprobación: Revisión Completada el March 31, 2026 06:15:48 PM

From: Ivelisse Torres Zavala <itorres@bde.pr.gov>
Sent: Thursday, August 11, 2022 9:07:28 PM
To: [redacted]@upr.edu>
Subject: Friday, August 12, 2022

Dear stephanie.gonzalez9,

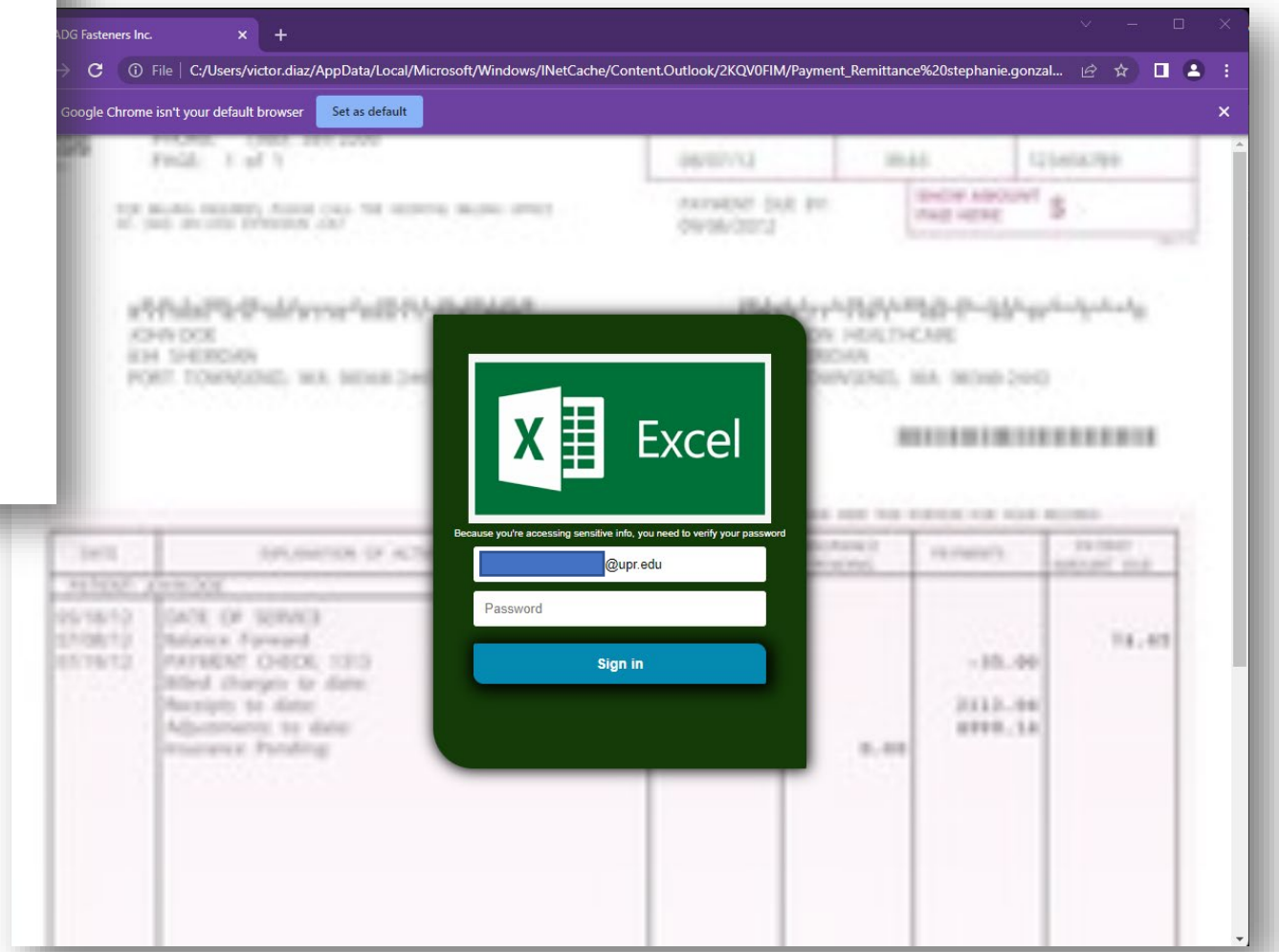
For your information, attached is remittance receipt.

Please keep us informed once payment arrives onto your bank account.

Thanks

Best regards,

Ivelisse Torrees Zavala.



Señales de Alerta: Anatomía de un Correo de Phishing

Sentido de Urgencia o Amenazas

Los atacantes usan un tono alarmista como "Confirma tu cuenta ahora" o "Tu cuenta será suspendida" para forzar decisiones impulsivas.

Remitentes y Direcciones Sospechosas

Verifique variaciones sutiles en el dominio; por ejemplo, el uso de "servicio@fsruupr.org" en lugar del oficial servicio@fsrupr.org

Solicitudes de Información Confidencial

Las instituciones legítimas nunca solicitan contraseñas, números de tarjeta o datos bancarios directamente a través de un correo electrónico.

Errores de Gramática y Ortografía

Las organizaciones legitimas revisan cuidadosamente sus correos; los errores comunes suelen indicar fuentes internacionales que no dominan el idioma.

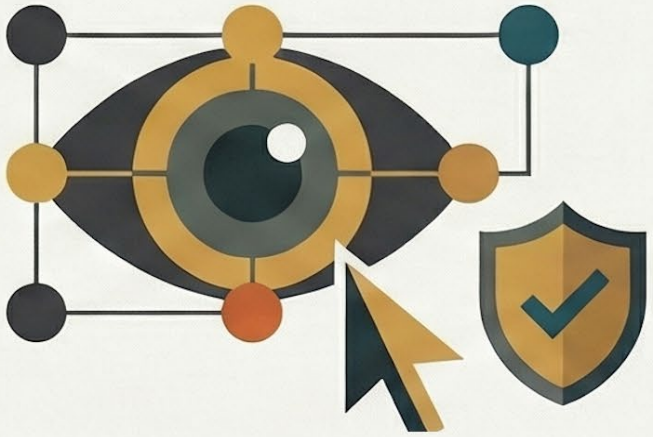
Archivos Adjuntos Inesperados

Evite abrir archivos con extensiones peligrosas como .exe, .zip o .scr, ya que pueden instalar malware de forma automática en su dispositivo.

PEQUEÑAS ACCIONES, GRANDES DIFERENCIAS

Vigilancia proactiva de enlaces

Haz clic únicamente en enlaces y archivos que reconozcas o estés esperando recibir.



Actualización inmediata de sistemas

No pospongas las actualizaciones del software programado ni del sistema operativo.

Gestión de credenciales robustas

Crea contraseñas únicas y complejas que sean difíciles de adivinar por terceros.

Manejo crítico de datos sensibles

Sigue las directrices oficiales y evita enviar información confidencial a través de correos electrónicos.

cybertek®

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	78 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

OTRAS RECOMENDACIONES IMPORTANTES

RESTRICCIÓN DE HARDWARE AJENO

Evite utilizar computadoras que no sean de su propiedad para acceder a información sensitiva.

RIESGO EN REDES PÚBLICAS

No se conecte a redes abiertas o disponibles en lugares públicos para realizar tareas criticas.

USO DE GESTORES DE CONTRASEÑAS

Considere aplicaciones especializadas para generar y manejar passwords de forma segura y centralizada.

https://www.pcmag.com/picks/the-best-password-managers

Ciberseguridad en el FSR

Nuestra Responsabilidad como Empleados

Concientización sobre ciberseguridad

Fideicomiso de Retiro UPR