1 de agosto de 2024

Un juego educativo gratuito ayuda a identificar y prevenir ciberdelitos

Invasión de los Estafaliens: un juego diseñado en Uruguay para prevenir los crecientes ciberdelitos y sobrevivir en el ciberespacio

POR **MAGDALENA CABRERA**

"Los **ciberdelitos** son la principal amenaza para nuestra región y también en Uruguay", con esta claridad y severidad se refirió Hernando Hernández, director de la Escuela Profesional de Seguridad del Instituto Securitas, acerca de la importancia de la ciberseguridad hoy.

Según un informe de Check Point Research, el área de investigación e inteligencia de Check Point Software Technologies, una empresa tecnológica multinacional proveedora a nivel global de soluciones de seguridad informática, el 2023 fue el año de los ataques de *ransomware*, y América fue la región que tuvo el mayor incremento en el último año.

LEÉ ADEMÁS


UNA BRECHA MULTICAUSAL
El camino en construcción de las mujeres en las tecnologías de la información
POR LEONEL GARCÍA SCAFFO


Futura regulación
Expertos advierten sobre riesgos del uso de inteligencia artificial para la vigilancia de personas en Uruguay
POR JOSÉ FRUGONI

En los ataques de *ransomware* los ciberdelincuentes cifran la información de las instituciones y luego piden dinero a cambio, para devolverla. En Uruguay fueron varias las organizaciones afectadas por este ciberdelito, e incluso muchos de ellos tuvieron notoriedad. "No ha quedado sector que no haya sido atacado", comentó a Galería Ethel Kornecky, catedrática de Ciberseguridad de la Universidad ORT Uruguay. "Si las empresas no tienen una buena política de *backup* y no tienen forma de restaurar esa información, tienen que pagar lo que les piden para desencriptar y descifrar los datos porque están ilegibles", explicó. El informe de Check Point Research advierte que una de cada 10 organizaciones en todo el mundo fueron afectadas por intentos de ataque de *ransomware* el año pasado.

Un informe anterior de la misma organización señala que en 2022 los ciberataques aumentaron un 38% respecto a 2021. En tanto, según datos que maneja la ONU, cada 39 segundos se produce un ataque informático en el mundo. Estos y otros datos, como el aumento en 2023 de un 75% en las intrusiones en la nube, según un informe de CrowdStrike, una empresa estadounidense de tecnología de ciberseguridad, fueron motivo más que suficiente para que en Uruguay un grupo de instituciones unieran esfuerzos para crear una herramienta educativa con el fin de concientizar sobre la importancia de estar protegidos en el mundo cibernético. Así nace Invasión de los Estafaliens, un juego educativo gratuito diseñado para aprender a identificar y prevenir estafas en línea.

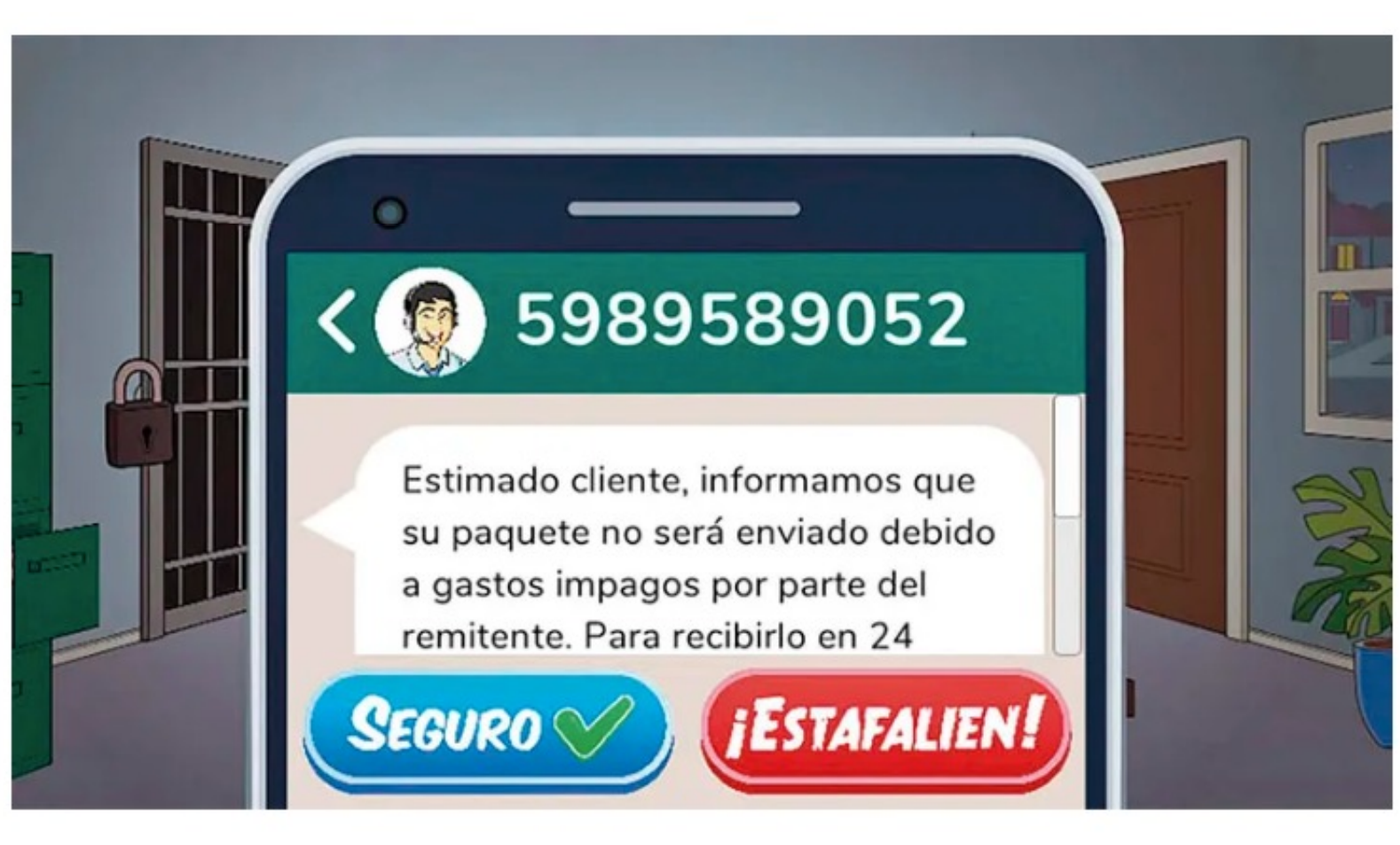
Estafaliens al ataque un juego diseñado para sobrevivir en el ciberespacio

Invasión de los Estafaliens es un proyecto de la Universidad ORT Uruguay, que contó con la colaboración de IBM, Securitas y el Banco República, y que se enmarca en el creciente esfuerzo por combatir el aumento global de ciberataques. La aplicación, lanzada recientemente, ya se encuentra disponible en Google Play y App Store. "Es una idea que se venía manejando en la universidad: generar un producto que fuera accesible a todo público y para todos los niveles, con el objetivo de educar a los niños, pero también a doña María y a don José, a todas esas personas que no tienen conocimiento de lo que son las estafas hoy en día en ciberseguridad", comentó Kornecky.

En Invasión de los Estafaliens, los jugadores asumen el papel de agentes especiales de la Agencia Virtual de Identificación de Vulnerabilidades Alienígenas Terrestre (Avivate), cuya misión es proteger a la Tierra de una legión de extraterrestres expertos en fraude y engaño, que se disfrazan de humanos para cometer las estafas. "Su premisa es que la jugabilidad sea sencilla, que sea cómico, accesible y atractivo para cualquier público objetivo. De hecho, tiene un ritmo de juego que se adapta a las capacidades de cada jugador. La idea es que no se tenga que tener ninguna experiencia previa para poder jugar", señaló la catedrática en Ciberseguridad de la ORT.

El juego tiene cuatro niveles iniciales, en los cuales el jugador debe resolver minijuegos basados en situaciones de la vida real que le enseñan a detectar y evitar estafas electrónicas. Una vez que pasa por todos ellos y obtiene el puntaje suficiente, queda habilitado para enfrentarse al Desafío Avivate, un nivel de supervivencia con más de 200 casos a resolver. Después de cada episodio, el juego emite un mensaje con buenas prácticas para crear conciencia. Por ejemplo, algún consejo sobre cómo utilizar las contraseñas, asunto sobre el cual se hace mucho hincapié, dejando claro que las mismas no se comparten.

Al respecto, Kornecky dijo que el juego trata de resolver casos de estafas con comunicaciones legítimas, como una comunicación telefónica o un mensaje de WhatsApp, que es lo que pasa todos los días. En cada caso aparece un número específico de estafaliens con diferentes nombres, que el jugador debe eliminar para proteger a la Tierra. Entre los estafaliens se encuentra, por ejemplo, Octopass, que rompe las contraseñas, y Urgencio, que convierte en urgente lo que es falso, de manera de forzar al usuario a contestar sin leer ni pensar demasiado. También está Confundio, que engatusa al usuario para que ingrese sus datos en sitios incorrectos.



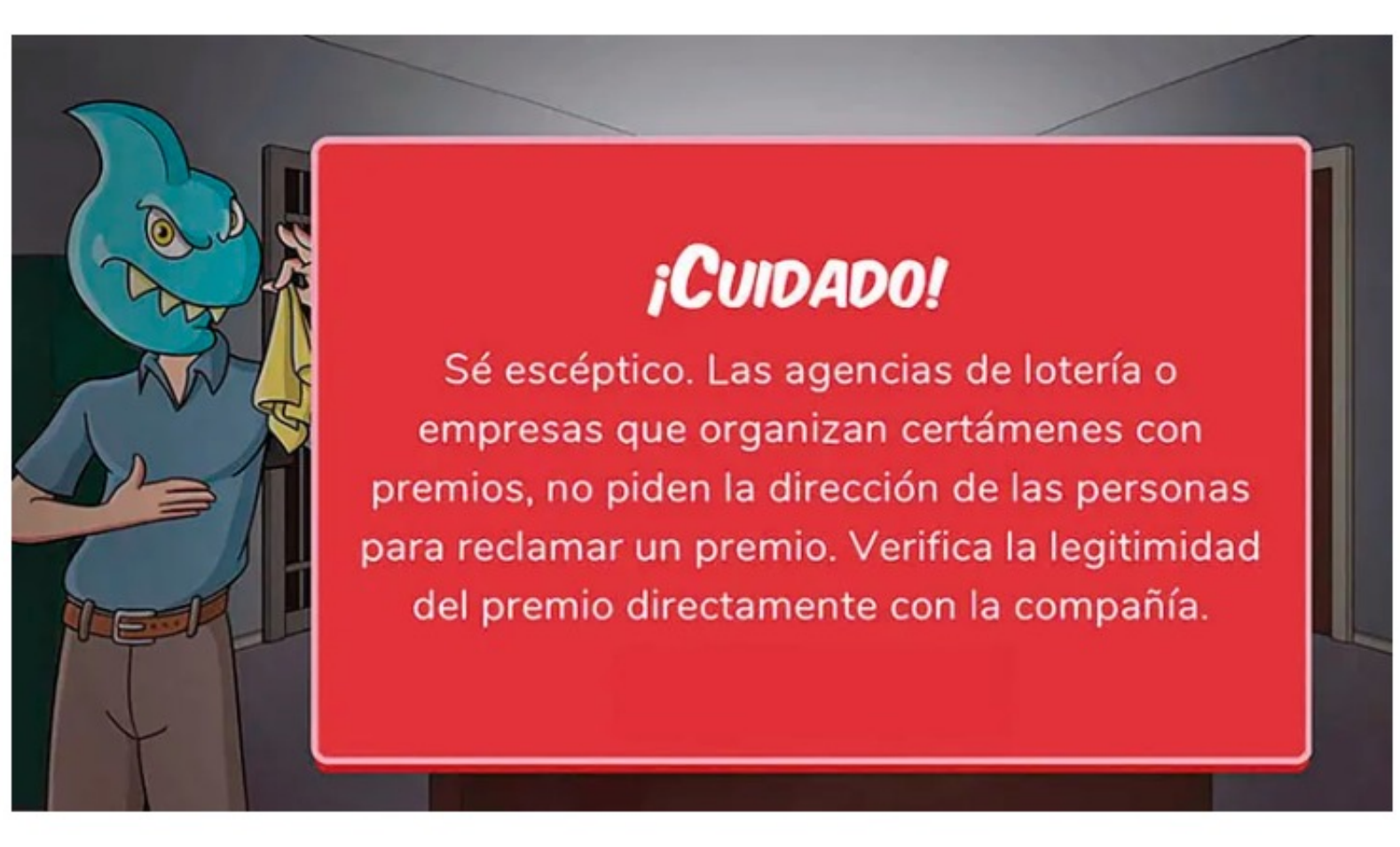
"La premisa del engaño es algo sobre lo que debemos educar permanentemente, dado que tiene una dinámica de cambio permanente. Los fraudes van en aumento año tras año", subrayó la catedrática en Ciberseguridad, agradecida por los apoyos recibidos para lanzar la primera edición del juego y para seguir avanzando con nuevas propuestas y mecánicas de estafa. Según adelantó, la idea a futuro es lanzar una nueva versión que incluya casos de delitos hechos a través de Mercado Pago. "Comprás algo que te sale 10 pesos y la persona en vez de 10, te tira 20 o 20.000. Ahí empieza un diálogo en el cual empezás a revelar un montón de información. Es un poco a donde queremos apuntar en la próxima versión", afirmó.

Los ciberdelitos crecen de forma exponencial

Hernández aseguró que en los últimos años han ocurrido "dos fenómenos muy importantes" que han acelerado el fenómeno de los ciberataques. Por un lado, la rápida convergencia de tecnologías que mejoró nuestras vidas, pero que al mismo tiempo nos dejó expuestos. A modo de ejemplo, mencionó los electrodomésticos inteligentes, que al estar conectados a internet, son posibles de monitorear, y el advenimiento de la inteligencia artificial. "Formulamos preguntas en internet, compartimos datos personales en las redes sociales, hacemos transferencias bancarias a través de wifi pública. Son muchísimas las vulnerabilidades que tiene un ciudadano y cualquier responsable de una organización en su privacidad".

El otro fenómeno que influyó en el crecimiento exponencial de los ciberdelitos fue la pandemia del Covid-19, ya que con ella cambió mucho el modo de trabajar y la educación. Hernández explicó que con el teletrabajo, por más que una empresa tenga un Departamento de IT que se dedique a monitorear los ciberdelitos, igualmente se encuentra muy expuesta, dado que el personal trabaja desde su casa y puede utilizar wifi público, su propio *mail* y nube, lo que dificulta todo tipo de control cibernético.

Según el informe de Check Point Research, en 2023 los sectores de actividad más afectados fueron la salud y la educación. La salud por tener información muy sensible, que roban y cifran para luego pedir mucho dinero para desencriptarla y devolverla. En la educación, el objetivo es el mismo y lo facilita la modalidad de educación a distancia.



Vulnerabilidades digitales uruguayas

En Uruguay los ciberdelitos más comunes son las extorsiones con contenido sexual, las estafas electrónicas, los falsos secuestros, la clonación de sitios web, el *phishing* (engaño haciéndose pasar por una persona, empresa o servicio) y el *ransomware*.

En este sentido, tanto Hernández como Kornecky coincidien en la importancia de educar en ciberseguridad desde la infancia. "Si logramos que los adolescentes entiendan estos temas, las futuras generaciones van a protegerse mejor", aseguró Hernández. Por su parte, a Kornecky le parece "genial que los niños tengan contacto con la tecnología, pero para eso hay que educar a los niños y a los educadores de forma transversal". Apuntó que el juego es "una forma de acercarlos, pero sin dudas necesitamos estar en la educación, con un proyecto educativo para las próximas generaciones. Si no educamos en etapas tempranas, tenemos realmente un problema".

La ORT se encuentra trabajando, junto con la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (Agesic), en una estrategia nacional de ciberseguridad para 2030 que incluirá a la Administración Nacional de Educación Pública (ANEP), al Ministerio de Educación y Cultura y a los demás organismos de la educación.

En tanto, Hernández llamó la atención sobre otra "vulnerabilidad" que tiene Uruguay: la falta de una ley de ciberdelitos, que ayude a combatirlos y a trabajar con el resto de los países. Al respecto, señaló que existe un proyecto de ley sobre el tema, pero continúa sin tratarse en el Parlamento. Explicó que esta ley se hace cada vez más necesaria, dado que actualmente los ciberataques están en manos de organizaciones, en las que existe una división del trabajo, cada persona se especializa en un tema y operan desde distintos países, ya no se trata de *hackers* aislados. "El combatir, prevenir y contribuir a la seguridad de los ciudadanos se hace muy difícil si no contamos con el marco legal para poder luchar con las autoridades de otros países. Ahí tenemos una vulnerabilidad importante", afirmó.

Los videojuegos, otro riesgo

Otro tema importante son los videojuegos. Para Hernández, "son utilizados en todo el mundo y también en nuestra región para reclutar y manipular psicológicamente a menores para cometer ataques de odio o para integrar organizaciones de crimen organizado". Quienes monitorean los videojuegos logran detectar a las personas que pasan más tiempo y que tienen un perfil más violento o más vulnerable, los reclutan y les hacen practicar los ataques sobre la base de una instalación real. Si bien en Europa se tiene más experiencia sobre esta realidad por el tema de los atentados, en América Latina hay organizaciones de crimen organizado que también reclutan gente con esta metodología.

Consejos de los expertos para una buena ciberseguridad:

No utilizar wifi pública para realizar transacciones o transferencias.

Si tenemos dudas sobre un mensaje que nos llega a través de las redes sociales, antes de realizar cualquier acción, llamar a donde corresponda (ejemplo, banco) y corroborar que la información sea cierta.

En los hogares, usar controles parentales para saber a dónde están accediendo los niños y adolescentes, pero hacerlo en conversación con ellos para irlos educando y formando en el tema.

Tener una contraseña o eslogan familiar, para evitar engaños. Por ejemplo, para saber si la persona que me está llamando por teléfono y pidiéndome el PIN de mi cuenta bancaria es realmente mi hijo o no.

TEMAS: CIBERDELITOS · URUGUAY · BROU

SECCIÓN SEMANAL

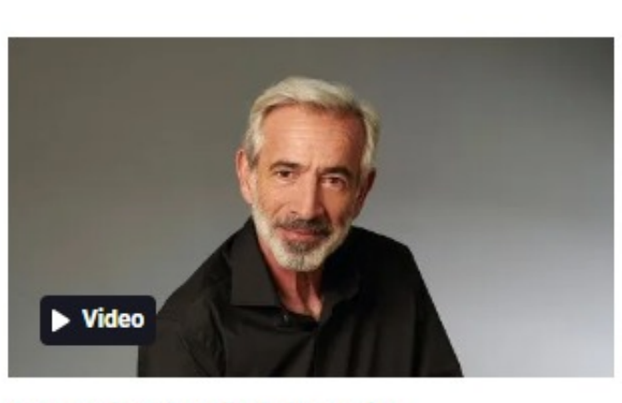
Energías renovables
Banco Mundial ve "potencial enorme" para el hidrógeno verde
POR ISMAEL GRAU

Seguridad
el predio del Penal de Libertad
POR JUAN FRANCISCO PITTALUGA

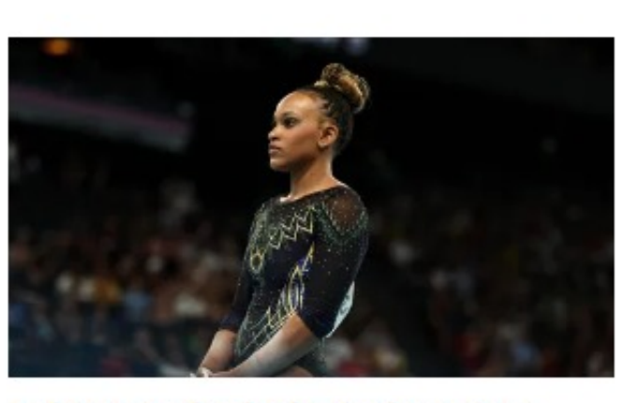
Contenedores
Oddone "no habría firmado" el acuerdo con Katoen Natie, aunque acepta la exclusividad en el puerto

Justicia
Tribunal de Apelaciones negó pedido de Fiscalía de extender prisión preventiva a imputado por violar a su hija
POR MACARENA SAAVEDRA

TE PUEDE INTERESAR



Imanol Arias:"Vivir en la incertidumbre ha hecho que el viejo no entre tanto en mí"
POR PATRICIA MÁNTARAS


Rebeca Andrade, la rival a quien Simone Biles ya traspasó su corona
POR MAGDALENA CABRERA


Cómo prevenir el abuso sexual infantil, según el libro Aprende a cuidar tu cuerpo
POR MARÍA INÉS FIORDELMONDO BLAIRES


El huerto de las brujas: un libro sobre las propiedades, los usos y las creencias en torno a las plantas