EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
01.09.2025	Dinero	1-7

EN EL REGRESO A CLASES

Ten cuidado con las estafas

Una de las temporadas del año en la que los cibercriminales lanzan más campañas maliciosas es el regreso a clases, como correos electrónicos falsos que usan logotipos y lenguaje institucional. Ten mucho cuidado.

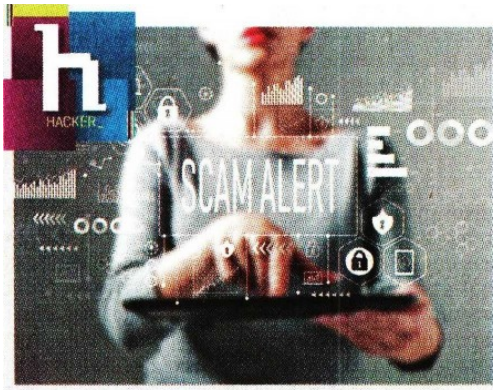


Foto: Especial

REGRESO A CLASES

PADRES Y ALUMNOS, EN LA MIRA DEL CIBERCRIMEN

Continúa en siguiente hoja

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
01.09.2025	Dinero	1-7

En esta temporada se usan diversas tácticas como ingeniería social, suplantación de identidad y falsificación de sitios web para atraer víctimas

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

El sector educativo es uno de los blancos favoritos de los cibercriminales, por eso, el regreso a clases es una de las estaciones donde lanzan más campañas maliciosas para adquirir nuevas víctimas y es necesario que tanto padres, como alumnos e instituciones estén alertas.

Este lunes 1 de septiembre, de acuerdo con el calendario oficial de la Secretaría de Educación Pública, regresan a clases cerca de 24 millones de niños y adolescentes de educación básica, lo que provoca que las familias gasten en útiles escolares, inscripciones, uniformes y dispositivos electrónicos.

Por lo anterior, la Asociación Nacional de Tiendas de Autoservicio y Departamentales estima que las familias gastan en promedio 7 mil 500 pesos para el inicio del ciclo escolar.

Para David González, investigador en Seguridad Informática del Laboratorio de Eset Latinoamérica, esto se convierte en un incentivo para los cibercriminales, quienes implementan diversas tácticas como ingeniería social, suplantación de identidad y falsificación de sitios web para atraer víctimas.

Resaltó que una de las campañas maliciosas que rondan durante el inicio del ciclo escolar es la suplantación de instituciones educativas.

Por ejemplo, envían correos electrónicos falsos que usan logotipos y lenguaje institucional para solicitar pagos inexistentes. De hecho, la Universidad Nacional Autónoma de México advirtió sobre mensajes que pedían depósitos por un costo de matriculación, el cual incluía amenazas de acciones legales si no se cumplía el pago.

A esto se añaden los sitios web falsos para venta de útiles, libros y uniformes, los cuales están diseñados para parecer tiendas legítimas, pero solicitan pago por adelantado y desaparecen tras recibir el dinero.

González explicó que los cibercriminales también aprovechan los programas del gobierno, por ejemplo, se hacen pasar por programas oficiales y piden datos bancarios para supuestamente transferir un apoyo económico.

"La urgencia por inscribir a un hijo o aprovechar una oferta especial hace que las personas bajen la guardia y no verifiquen la autenticidad del mensaje o sitio web", resaltó.

Además, no sólo los padres de familia son engañados. También se enfocan en alumnos más allá del nivel básico.

Un ejemplo es que publican ofertas laborales fraudulentas para estudiantes a quienes se les requieren pagos para "procesar" el empleo o solicitan datos bancarios bajo pretexto de depósito de nómina.

Sin olvidar las estafas de renta de vivienda, es decir, publican en internet espacios o cuartos atractivos para estudiantes, piden el depósito por adelantado y el lugar nunca existió.

¿Y LAS INSTITUCIONES?

Una investigación de Check Point Research encontró que las instituciones educativas también se mantienen como un blanco atractivo para el cibercrimen.

Esto porque, tan sólo de enero a julio de este año, el sector en México registró 4 mil 188 intentos de ataque a la semana, lo que representa un aumento del 19% interanual.

Miguel Hernández y López, gerente general de Check Point Software en México, detalló que el método favorito para atacar a las instituciones es el phishing, ya que a nivel global se detectaron 18 mil 391 nuevos dominios relacionados con escuelas y universidades, siendo uno de cada 57 malicioso o sospechoso.

Muestra de ello es que había páginas de inicio de sesión universitarias falsas que imitaban a Outlook y estafas con códigos QR.

"El sector educativo se está convirtiendo en la zona cero de los ciberdelincuentes, con un aumento repentino de los ataques a medida que los estudiantes y el personal están más activos en línea", advirtió.

Ambos expertos consideraron que se debe adoptar un enfoque preventivo

Continúa en siguiente hoja

para garantizar la seguridad de las escuelas, los alumnos y las futuras generaciones.

LOS DATOS RECOMENDACIONES DE SEGURIDAD:

- Verificar los remitentes y dominios de los correos electrónicos antes de hacer clic en cualquier enlace o realizar pagos.
- Realizar las compras únicamente en sitios web oficiales o en comercios reconocidos.
- Evitar acceder a enlaces compartidos en redes sociales que no cuenten con respaldo o referencias comprobables.

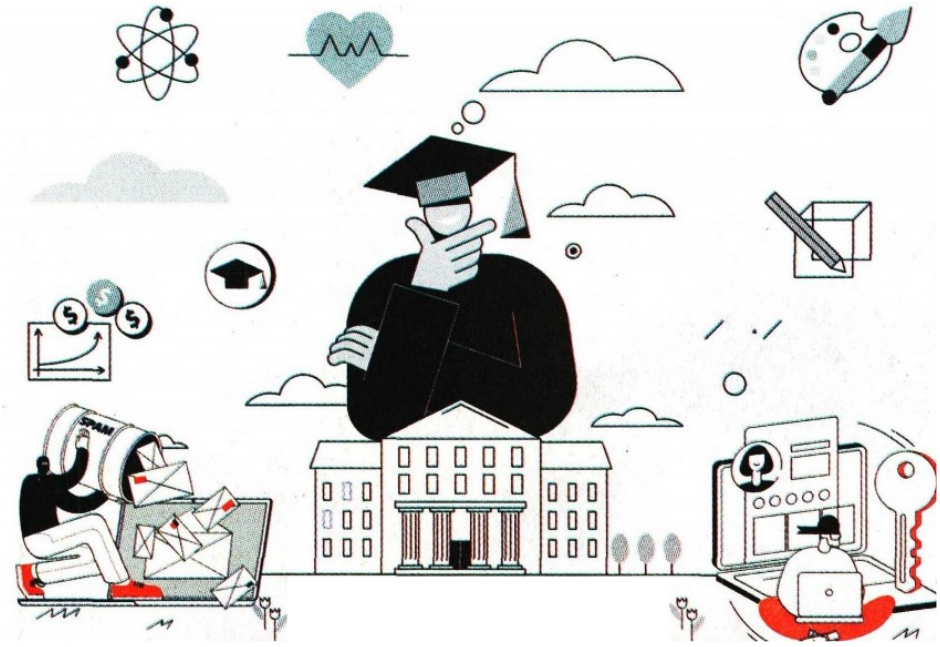
La educación digital juega un papel fundamental, ya que enseñar a padres, maestros y alumnos a identificar señales de alerta y es tan importante como capacitarlos en el uso de herramientas tecnológicas básicas"

DAVID GONZÁLEZ
INVESTIGADOR EN

SEGURIDAD INFORMÁTICA DEL LABORATORIO DE ESET LATINOAMÉRICA

Las instituciones deben adoptar defensas por capas, priorizar la concienciación sobre el phishing y aplicar la autenticación multifactor."

MIGUEL HERNÁNDEZ Y LÓPEZ
GERENTE GENERAL DE CHECK POINT SOFTWARE EN MÉXICO



Fotos: LinkedIn / Gráfico: Especial