LITORALPRESS

Fecha: 09-07-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: Las claves para evitar ataques digitales a funcionarios chilenos

Pág. : 4
Cm2: 354,6

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Capacitación, monitoreo y equipos de ciberseguridad:

Las claves para evitar ataques digitales a funcionarios chilenos

Las autoridades son más atractivas para que los *hackers* suplanten su identidad.

MANUEL HERNÁNDEZ

Solo el 0,1% de las personas puede detectar un video, imagen o audio falso, creado o manipulado con IA (conocido como *deepfake*). Así lo confirma un estudio de iProov, uno de los principales proveedores en el mundo de soluciones para la verificación biométrica de identidad. El análisis evaluó a 2.000 usuarios de Reino Unido y EE.UU.

El profesor Edgar Whitley, experto en identidad digital de la London School of Economics and Political Science afirma que los expertos en seguridad "llevan tiempo advirtiendo de las amenazas que suponen los *deepfakes* tanto para las personas como para las organizaciones".

Con ese antecedente, los funcionarios chilenos también podrían ser blancos de ataques. Martina López, investigadora de seguridad informática de ESET Latinoamérica, explica que "este tipo de intentos de daño por parte de ciberatacantes se apoya muchísimo en el engaño hacia la persona". Por eso, dice que más allá de las herramientas en seguridad o inversiones en presupuesto de Estado en ciberseguridad, "la conciencia (de los funcionarios) resulta mucho más importante que tener las herramientas más actualizadas para poder prevenir este tipo de ciberataques".

OPCIONES

En caso de dudas, usar herramientas y acordar palabras clave entre colegas puede ayudar a confirmar la identidad.

La especialista recalca que Chile es un país avanzado a nivel regional en materia de ciberseguridad, pero en este caso lo más importante es que los funcionarios estén capacitados, de forma "periódica, actualizada, y que les informen que para muchos atacantes ellos van a ser el blanco, con nombre y apellido", ya que será más sencillo engañar a una persona con un audio falso, un chat falso, un correo electrónico, un enlace al ingresar o un archivo adjunto malicioso.

López detalla que a nivel organizacional también es clave utilizar herramientas de monitoreo que emitan alertas en caso de algún movimiento sospechoso y que puedan mitigarlas de forma automática. Además, agrega, es relevante contar con un equipo de ciberseguridad "que controle este tipo de herramientas, así como soluciones de autenticación, que no sean optativas, que sean obligatorias".

Y concluye que no hay herramienta ni presupuesto en seguridad "que impida que una persona distraída simplemente haga click, entregue algún tipo de información o descargue algún archivo malicioso".

Pete Nicoletti, director de seguridad de la información de Campo Global en Check Point Software, coincide y explica que las suplantaciones de identidad son "campañas de información maliciosa", ya que buscan establecer "narrativas manipuladas para engañar y desestabilizar".

¿Cómo evitarlo? Según Nicoletti, con una solución robusta de Gestión de Riesgos Externos (ERM), que incluye "usar palabras clave previamente acordadas y compartidas fuera de banda antes de las reuniones, y durante las videollamadas", además de pedir a los participantes que muestren la parte posterior de la cabeza, ya que es una zona que la IA actual tiene dificultades para replicar.

También menciona herramientas como www.facechecck.id, que "pueden ayudar a detectar el uso no autorizado de tu imagen", pero aclara que lo más relevante es "educar a las personas para que reconozcan y respondan a estas amenazas".

RAÚL BRAVO

LA SUPLANTACIÓN de identidad busca generar "narrativas manipuladas para engañar y desestabilizar", según expertos.