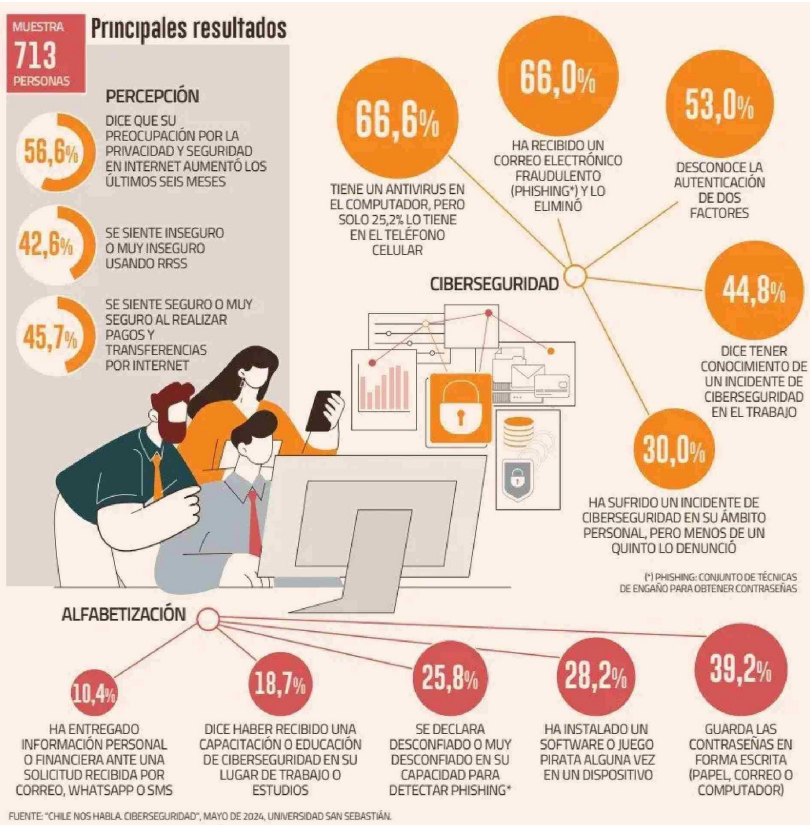
LITORALPRESS

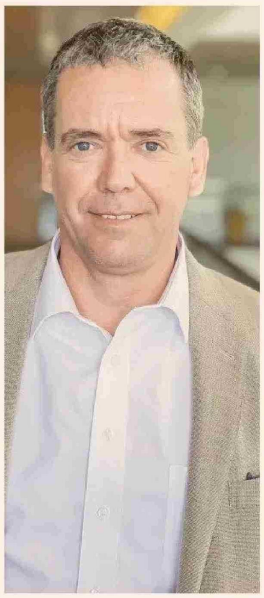
Fecha: 31-05-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Felipe Harboe: "En Chile necesitamos un proceso profundo de alfabetización digital"

Pág. : 40
Cm2: 666,5
VPE: $ 5.905.874

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida



FUENTE: "CHILE NOS HABLA. CIBERSEGURIDAD", MAYO DE 2024, UNIVERSIDAD SAN SEBASTIÁN.



Felipe Harboe: "En Chile necesitamos un proceso profundo de alfabetización digital"

A raíz de la encuesta Chile Nos Habla, sobre ciberseguridad, de la Universidad San Sebastián, el abogado e investigador enfatizó en la necesidad de educar a la ciudadanía en la materia y también se refirió al impacto del cibercrimen organizado en las empresas.

POR MARCO ZECCHETTO

La exposición a las redes sociales y los riesgos asociados a la seguridad informática se han transformado en una preocupación para los chilenos. Así lo concluyó la encuesta Chile Nos Habla, de la Universidad San Sebastián (USS), -realizada entre el 26 de abril y el 15 de mayo de 2024-, la que abordó las percepciones, preocupaciones y experiencias de los chilenos en ciberseguridad.

Entre sus principales hallazgos, el 94,3% de las personas declaró haber recibido correos electrónicos o mensajes sospechosos de *phishing* o fraude; 56,6% dijo que su preocupación por la privacidad y seguridad en Internet aumentó en los últimos seis meses; y en el ámbito laboral, un 44,8% conoce o ha sabido de un ataque o incidente de ciberseguridad en su trabajo.

Ante esto, el investigador del Centro de Estudios en Seguridad y Crimen Organizado (Cescro) de la USS, y socio de H&Co Abogados, Felipe Harboe, dijo que estos resultados demuestran que, aunque el conocimiento y percepción de la ciberseguridad ha ido creciendo en el país, "todavía es insuficiente".

"En Chile necesitamos un proceso profundo de alfabetización digital, no solo para conocer las bondades de las redes y de la informática, sino también para conocer sus riesgos", afirmó.

Responsabilidad tripartita

Consultado respecto de quién tiene la responsabilidad de educar a las personas en ciberseguridad, afirmó que es compartida entre el Estado, los empleadores, y la ciudadanía.

"Aquí hay una obligación tripartita. Además de todas las regulaciones que está adoptando el nuevo ecosistema jurídico de la economía digital, el Estado debe crear espacios de alfabetización, por ejemplo, *spots* de televisión que enseñen a la gente cómo prevenir y cómo reaccionar", dijo Harboe.

A nivel empresarial, comentó que es necesario que los empleadores "entiendan que la ciberseguridad debe ser un asunto de gobierno corporativo, y que no está sólo restringido al ámbito informático o del *compliance* (cumplimiento normativo)".

Afirmó que hoy muchas organizaciones no tienen conocimiento de los datos que manejan, ni de los riesgos asociados a sus operaciones de ciberseguridad, y que deben tomar medidas. Entre ellas, realizar informes de brechas de incumplimiento ante seguridad informática, invertir en la capacitación de sus trabajadores, y regularizar procesos internos en materia de protección de datos para avanzar en prevención y mitigación de incidentes.

Harboe señaló que también existe una responsabilidad en la ciudadanía de informarse sobre los riesgos a los que están expuestos y cómo prevenirlos, además de adoptar medidas de resguardo asociadas, por ejemplo, al manejo de contraseñas y el uso responsable de redes sociales.

"Al observar víctimas de estafa o ciberataques, se puede ver que muchas de estas ocupan regularmente redes *wifi* públicas para hacer transacciones bancarias, utilizan la misma clave para todas sus cuentas e, incluso, entregan los datos de sus tarjetas en redes sociales o sitios no seguros. Hay mucha preocupación, pero poca ocupación por parte de las personas", comentó.

Cibercrimen organizado

Harboe afirmó que Chile se ha transformado en un país "muy atractivo" para el cibercrimen organizado, porque cuenta con "la economía más digitalizada de América Latina y un desarrollo tecnológico bastante más elevado que los países vecinos".

Explicó que el problema radica en que la digitalización de procesos no ha ido de la mano con la evolución de la inversión en ciberseguridad, lo que ha despertado el interés de bandas organizadas en perpetrar sus ataques en el país.

"El costo promedio de un ataque en Chile supera los US$ 1,2 millones. Es un daño patrimonial importante para las empresas y por eso es relevante que la institucionalidad pública y el mundo privado se coordinen para tener mecanismos preventivos, y en eso va a aportar mucho la nueva Ley Marco de Ciberseguridad", dijo Harboe.

Según el abogado, estas bandas han orientado sus ataques a las empresas principalmente a través del bloqueo o denegación de servicios, además de la sustracción de información privada de las organizaciones, la que posteriormente es comercializada en el mercado negro, o se utiliza como extorsión a cambio de un rescate económico.

"Muchas veces las empresas tienen una linda política de privacidad, pero que en la práctica no opera, y eso es un problema. Además, debe existir conocimiento de este tema en los directorios. Todo lo que se invierte en publicidad y en construcción de marca puede destruirse por un daño reputacional derivado de un incidente de ciberseguridad mal manejado", afirmó.*