



DAVID VELASQUEZ

38% de los latinoamericanos aún no sabe distinguir un email verdadero de uno falso

APRIL NUÑEZ

Robo de bases de datos, clonaciones, mensajes fraudulentos y más son solo la punta del iceberg de ataques informáticos que ponen en jaque tanto la seguridad de particulares como de las empresas. Por eso cada vez son más solicitados los especialistas en ciberseguridad.

"Se evidencia la necesidad urgente de profesionales que apoyen a organizaciones para evitar brechas de seguridad significativas, disminuyendo el riesgo de discontinuidades operacionales, en los distintos ámbitos de la sociedad", comenta Javier Navarro, vicerrector de Admisión y Desarrollo Estudiantil de U. de las Américas, institución que a partir de este año impartirá la carrera de Ingeniería en Ciberseguridad 100% online con una duración de 8 semestres.

Su meta, dice Navarro, es aportar a la urgente transformación digital de empresas de todos los tamaños, servicios públicos y un sinnúmero de entidades, proceso acelerado por la pandemia. "La carrera forma profesionales enfocados en resguardar la continuidad operacional y mantener un nivel adecuado de protección de la información de la organización, garantizando la integridad, confidencialidad y disponibilidad de los datos, sistemas e infraestructura tecnológica", resume. Más info en [udla.cl](https://bit.ly/3hWQYI8) (<https://bit.ly/3hWQYI8>).

Los correos raros

El phishing o robo de identidad es una de las ciberataques más comunes: los delincuentes sustraen datos personales para acceder a cuentas

Consejos de expertos en ciberseguridad para teletrabajar sin exponerse

Universidades ya forman especialistas en prevenir ataques informáticos: la UDLA estrena la carrera el 2021.

Contraseñas vs. algoritmos

Con el boom del comercio online, muchos están creando cuentas en montones de sitios. ¿Conviene dejar todas las contraseñas guardadas en el celular o computador? "Ahora que está muy de moda comprar a un clic, lo mejor es cerrar sesión, no usar las mismas contraseñas y evitar crearlas con datos personales: los algoritmos captan eso rápidamente", aconseja José Ignacio Cardona, coordinador académico de Ingeniería en Ciberseguridad de la Universidad Mayor. En su plantel la carrera se dicta online y tiene una duración de 6 semestres. Más info en [umayor.cl](https://bit.ly/39fWcV5) (<https://bit.ly/39fWcV5>).

bancarias o números de tarjetas de crédito; su meta es defraudar a los usuarios que regularmente caen en sus trampas a través de correo electrónico, mensajes o vía WhatsApp.

¿Cómo detectarlos? "Algunos son fáciles de detectar, ya que inclu-

yen errores ortográficos, gramática descuidada, gráficos poco profesionales y saludos demasiado genéricos", detalla Roberto Martínez, analista senior de seguridad en Kaspersky. ¿Parece un consejo repetido? No tanto: esta compañía global

de ciberseguridad, en conjunto con la consultora de estudios de mercado Corpa, realizó una investigación que reveló que en promedio 38% de los latinoamericanos aún no sabe distinguir un email verdadero de uno falso (puede ver el estudio acá: <https://bit.ly/39bBHc6>).

Ojo entonces con los correos raros. "En especial con los que parecen provenir de entidades oficiales y comunican una urgencia, una oferta disponible a un número limitado de usuarios o amenazan con multas si no se toma la acción requerida a la mayor brevedad", ilustra Martínez.

"La mayoría de los casos de phishing se deben a que las puertas de entrada a los espacios informáticos no fueron cubiertos o errores en la programación. Lo otro que se ha visto en este último tiempo son los ransomware (secuestros de información). Se infiltran en los sistemas, los toman y bloquean hasta que paguen

una fianza de rescate por el acceso de vuelta a la información", explica Francisco Kemeny, CEO de Roier.ai y especialista en transformación digital.

Una navegación segura

Con tanta gente trabajando y/o estudiando desde casa, las puertas de entrada de los ladrones digitales se han multiplicado. No es lo mismo, claro, mantener altos estándares de ciberseguridad en una oficina que en una red de cientos de computadores desperdigados por la ciudad.

¿Cómo prevenir ciberataques a nivel doméstico? Bruno Calderón, CEO de servicios digitales Springs Digital, recomienda de partida instalar un antivirus en el PC y mantenerlo actualizado.

"Utilizar una contraseña segura para la red wifi, cambiando las claves genéricas de routers y módems en las redes domésticas. Nunca enviar claves y utilizar respaldos de archivos en la nube a través de proveedores reconocidos como Google, Office 365 o iCloud de Apple", agrega Navarro