Ciberseguridad: un aprendizaje necesario

¿Conoces a alguien que ha sido victima de una estafa digital?

Vaciamiento de cuentas bancarias; robo de usuario de WhatsApp para pedir dinero a tus contactos; terceros informando falsos secuestros o problemas de familiares que demandan pago urgente de dinero, mails falsos de entidades bancarias, son algunas de las situaciones más comunes que hemos venido escuchando en los últimos tiempos.

La tecnologia facilita la comunicación, la vida laboral y optimiza tiempos, pero también nos expone. Y es que en estos tiempos en que vivimos, cada vez más dependientes de la tecnología, los riesgos de ciberataques también pasaron a ser parte de la vida diaria. No hace falta trabajar en grandes empresas o bancos para verse afectado: hoy cualquiera puede recibir un mensaje engañoso o ser víctima de un fraude digital.

¿Estás expuesto a ciberataques?

Phishing

Uno de los casos más habituales es el de los mensajes falsos, conocidos como “phishing”. Seguramente te llegó un SMS o correo electrónico avisando que tienen un paquete retenido, supuestamente del Correo Uruguayo. El mensaje suele generar apuro y pide hacer clic en un enlace y realizar un pago. ***Como regla básica, no confies o respondas mensajes de que te exigen respuestas urgentes o te piden que entres a un link y ante la duda, contacta directamente al organismo.***

Supuestos pagos erroneos

Una estafa habitual que muchas veces se asocia a compras o ventas on line. El supuesto comprador manifiesta haber hecho una transferencia por un monto mayor al que correspondía y manifiesta que “contactó al banco” y señala que desde la institución le pidieron que la devolución se realice a través de un link determnado. El ingreso al link les permite acceder a tu cuenta bancaria y a partir de allí se produce la sustracción. ***En este punto conviene tener presente el evitar el acceso a links que nos remitan por mensaje y entrar al sitio del banco para verificar la información.***

Estafas directas

También están los engaños más directos, donde alguien se hace pasar por otra persona (el famoso cuento del tío). Puede ser un supuesto técnico que ofrece ayuda, un “compañero de trabajo” o incluso alguien que dice ser un jefe pidiendo una transferencia urgente. ***En estos casos, lo más importante es no actuar con apuro: ante pedidos sensibles, siempre es recomendable tomarse un tiempo, razonar lo que nos piden, confirmar por otro medio, como una llamada o un mensaje independiente.***

Contraseñas

Otro punto débil muy común son las contraseñas. Muchas personas usan la misma clave para todo o eligen combinaciones fáciles de recordar, como fechas o nombres. El riesgo es que, si alguien accede a dicha contraseña, puede abrir la puerta a otras cuentas. ***Una buena práctica es usar contraseñas distintas para cada servicio, robustas (con mayúsculas, números, caracteres, etc.) y difíciles de adivinar, o apoyarse en aplicaciones que las gestionan de forma segura.***

Lo importante es entender que estos problemas no aparecen por separado. Un mensaje falso puede servir para robar una contraseña, y con esa contraseña luego hacerse pasar por la persona para engañar a otros. Por eso, una práctica clave

es activar un segundo factor de autenticación en las cuentas más importantes, lo que agrega una capa extra de protección incluso si la contraseña se ve comprometida.

En el trabajo, estos riesgos pueden tener consecuencias mayores. En empresas u oficinas, donde se manejan pagos o información importante, un simple descuido puede terminar en una pérdida económica o en la exposición de datos sensibles. Incorporar hábitos como validar solicitudes inusuales, ***no compartir claves y seguir procedimientos claros ayuda a reducir significativamente estos riesgos.***

En el día a día, pequeños cuidados marcan la diferencia.

Mantener los dispositivos actualizados, tener un antivirus eficiente, evitar actuar por impulso ante estos pedidos y prestar atención a los detalles de los mensajes (errores, direcciones raras, pedidos urgentes) son acciones simples que previenen muchos problemas. La mayoría de los ataques se aprovechan de distracciones más que de fallas técnicas complejas.

La seguridad en internet no es solo un tema de expertos.

Es una cuestión de hábitos. En un país tan conectado como Uruguay, incorporar estas buenas prácticas permite reducir riesgos y usar la tecnología con mayor tranquilidad, aprovechando sus beneficios sin quedar expuestos

En ALTERNOVA colaboramos tanto con empresas como con personas a prevenir estas situaciones, identificando riesgos, brindando capacitación práctica y diseñando soluciones de seguridad digital accesibles que protegen la información, el patrimonio y la tranquilidad en el uso cotidiano de la tecnología.

CIBERSEGURIDAD ENFOCADA A EMPRESAS

A nivel de PYMES los riesgos crecen, las empresas deben proteger sus activos, gestionar los riesgos, fortalecer sus defensas.

Una buena política en esta área debería:

· Identificar y gestionar los riesgos de tu información.

· Mejorar continuamente la seguridad y el cumplimiento.

· Involucrar a toda la empresa en una cultura de protección de su sistema de informaciòn.

· Mantener políticas claras en materia de seguridad de la información accesibles y sostenibles.

Desde ALTERNOVA trabajamos para que las PYMES accedan a Consultorías en materia de Seguridad de la Información accesibles y a medida. Implementamos sistemas de seguridad definidos, documentados y comprendidos por toda la Organización.

Dr Pablo Bicudo