Buena Vida

Editora: Lucrecia Choy.

Informarse sobre temas de seguridad digital es una manera de estar prevenido.

En el mundo se ha registrado un aumento en la ola de ataques cibernéticos. Prevenga.

FOTO PRENSA LIBRE: OTTONBRO/PEXELS

Cuán vulnerables somos a los ataques cibernéticos

Martes tecnológico

Por Ingrid Reyes
ireyes@prensalibre.com.gt

Al parecer la evolución de la tecnología permite que exista también un problema mayor de amenazas informáticas, ya que los ataques a diario crecen en complejidad y se hacen también más sofisticados. Esto no quiere decir que tengamos temor de utilizar la tecnología, pero sí es importante tomar algunas medidas para prevenir y conocer más cómo cuidar nuestra información.

Miguel Mendoza, Security Researcher en ESET Latinoamérica, explica que ellos a diario encuentran cerca de 450 mil nuevas muestras únicas de malware, es decir que se incluye todo tipo de software malicioso, algunos de ellos como los troyanos (después de introducirse en el dispositivo objetivo, emplean varias técnicas para ser ejecutados por el usuario u otro software en el sistema afectado de manera inconsciente); *ransware* (secuestro de datos por los que hay que pagar cierta extorsión); virus (infiltración que daña los archivos existentes en el equipo); gusanos (programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red); y *malware* de banca.

En septiembre de 2020 se registró la primera muerte asociada con un ciberataque, recuerda Mendoza. Una paciente que necesitaba cuidados intensivos tuvo que ser trasladada cuando los sistemas del Hospital Universitario de Düsseldorf en el que se encontraba dejaron de funcionar por un ataque ransomware. La policía alemana atribuye su muerte a los piratas informáticos.

CUIDAR LA INFORMACIÓN

Estos ataques han crecido no solo por el avance tecnológico sino porque ha existido evolución en la astucia de los ciberdelincuentes en sus ataques esto principalmente por situaciones críticas como la pandemia, explica Melinton Navas, profesional de seguridad de la información y actual jefe de seguridad de Xoom, A PayPal Service. "La pandemia ha habilitado a estos ciberdelincuentes para inspirar nuestras estrategias de estafas para los usuarios", dice.

Unity Willis Towers Watson registra que solo durante la primera mitad del 2020 se registraron más *ransomware* que todo el 2019. El 34% de las empresas afectadas tardaron una semana o más en recuperar el acceso a sus datos y se espera que una empresa sea atacada cada 11 segundos para finales del 2021.

Luis Flores, Gerente General de Unity Willis Towers Watson Guatemala comenta que según un estudio reciente realizado en esta institución, se ha detectado que hay debilidades y vulnerabilidades en las compañías como: falta de planes de respuesta a incidentes; el comportamiento de los colaboradores por desinformación en cuanto a la ingeniería social, el uso de los dispositivos propios y el manejo de páginas y aplicaciones inseguras, entre otros aspectos relevantes a lo que es necesario darle seguimiento para fortalecer la seguridad de la empresa.

En la actualidad Flores explica que existe una póliza de seguros a nivel empresarial para apoyar en servicios de informática forense y recuperación de datos, servicios legales, gastos de restitución de imagen, entre otros detalles que enfrentan las empresas.

A NIVEL PERSONAL

Mendoza refiere que el ideal es que cada uno sea más consciente y responsable para aprovechar la tecnología, seguir ciertos parámetros para evitar que personas mal intencionadas consigan su objetivo.

Navas recomienda prestar atención al sentido común, "las tecnologías pueden protegernos hasta cierto punto y no existe una por el momento que pueda protegernos de todo, así que nosotros debemos asumir el papel como usuarios de responsabilizarnos (...) si recibo una comunicación extraña que pretende ser de mi entidad financiera o banca en línea, prefiero escribir manualmente la url de la entidad para confirmar lo que dice el correo, pero no hago click a los enlaces", explica.

Cuando ocurre un episodio de estos, la recomendación principal de Navas es acudir a la entidad por medio de la cual nos desfalcaron información o dinero, ellos tienen más poder para eliminar la estafa o amenaza. Si es un caso muy grave se hace la denuncia en el Ministerio Público, así queda un registro histórico. Y si en un futuro existiera algún problema por el robo de identidad, esta información verifica que sufrimos el ataque", agrega Navas.

+ PREVENCION

"El antivirus hace una parte de la protección, pero la otra parte queda en nuestra responsabilidad y consiste en no visitar páginas de dudosa procedencia, no seguir enlaces en redes sociales que no sean confiables y llamen a hacer acciones. Esto funciona a todo nivel", afirma Melinton Navas, profesional de seguridad de la información y actual jefe de seguridad de Xoom, A PayPal Service.
Los usuarios y contraseñas tampoco deben ser compartidas, "en ocasiones se piensa que la entidad financiera debería conocer también estos detalles, pero esto no es cierto, ninguna tercera persona debería saber esos datos", concluye el experto.

¿CÓMO LOGRAR MÁS SEGURIDAD?

Los expertos destacan algunas medidas ideales para tener en cuenta en el uso de la tecnología.

- **Mantenga un software** de seguridad adecuado y actualizado. Esto permite protegerse de la mayoría de los posibles ataques. Las soluciones de seguridad alertan y orientan cuando se está poniendo en algún riesgo.
- **Evite abrir** páginas dudosas, así como links o archivos de remitentes desconocidos.
- **Si no ha** participado en un concurso, dude de cualquier correo que reciba diciendo que usted ha sido ganador de premios.
- **Utilice diferentes** contraseñas en cada servicio. Busque que estás sean únicas y robustas, esto evita que los criminales tengan la facilidad de entrar a otros servicios.
- **No comparta** la contraseña con ninguna persona o institución. Esto es información personal.
- **Use el doble** factor de autenticación cada vez que sea posible. Esto hace que el usuario reciba un código en su teléfono celular cuando ingresa a una cuenta propia y si alguien más está intentado entrar es importante que cambie la contraseña lo antes posible.
- **De preferencia** utilice solamente conexiones wifi de confianza, en especial cuando verá información sensible o financiera.
- **Mantenga actualizadas** las aplicaciones y el sistema operativo. Las aplicaciones y sistemas operativos están constantemente haciendo mejoras en la seguridad.
- **Edúquese** en temas de seguridad para prevenir.