En la actualidad, con el desarrollo vertiginoso de las Tecnologías de la Información y Comunicación (TIC), se ha manifestado una tendencia hacia el crecimiento del desarrollo de aplicaciones, que en dependencia del tipo de negocio al que estén asociadas, se inclinan o no al procesamiento de grandes volúmenes de datos. Paralelo al desarrollo de las TIC crece la necesidad de la seguridad de la información que es generada, almacenada, intercambiada y procesada. Las tendencias mundiales revelan un crecimiento exponencial de acciones malignas encaminadas a poner en riesgo la seguridad de la información.

Desafortunadamente, ninguna entidad es inmune a estas acciones malignas, por lo que deben implementar un plan ordenado de prevención, con el objetivo de reducir los riesgos ante una exposición directa. En Cuba, se trabaja arduamente para informatizar los procesos en todas las ramas de la sociedad y adaptarse a la revolución tecnológica y constante existente en este sentido a nivel mundial. Motivo por el cual en los últimos años se han aprobado diversas leyes que regulan el comportamiento que deben tener los usuarios en el ambiente virtual, dinámico y retador conocido como ciberespacio.

Ahora bien, la gran dependencia de la tecnología para la protección contra amenazas cibernéticas en constante evolución ignora muchas veces el elemento más crítico: el factor humano. Es por eso que le brindamos un grupo de sugerencias que aseguran pasos firmes de los usuarios en el mundo digital. Los datos personales constituyen el

tesoro más valioso que tiene un usuario en la red, por lo que siempre es necesario ponerlos en buen resguardo. De ahí que:

1. Conéctate solo a redes privadas, principalmente, cuando manipules información privada o confidencial.
2. Protege todos tus dispositivos con un código alfanumérico de identificación personal (PIN o contraseña), utilizando para ello patrones seguros e indescifrables y una diferente para cada cuenta.
3. Activa siempre que sea posible la verificación de dos pasos (2FA, según sus siglas en idioma inglés Two Factor Authentication); lo que implica añadir un paso adicional al proceso de autenticación de usuarios, con la misión de comprobar la autenticidad de quién está accediendo a un sistema informático.
4. Realiza copias de seguridad constantes de tus datos.
5. No debes abrir correos electrónicos o archivos adjuntos enviados desde direcciones desconocidas. Los mensajes de phishing se difunden mediante el uso de correos electrónicos, SMS, mensajes instantáneos, sitios de redes sociales, entre otros. Según la empresa consultora y de investigación de las tecnologías de la información, Gartnert Inc., el 65% del total de estos ataques se realiza mediante el envío de hipervínculos maliciosos dentro del correo electrónico.
6. Debes tener mucho cuidado con la información que compartes en las redes sociales, blogs, foros de opinión o cualquier otra plataforma de acceso público.

De Cubadebate.