Cinco consejos clave para no ser víctima de ciberataques

Existe un proceso acelerado de digitalización, las actividades han migrado al mundo virtual, acortando distancias y agilizando procesos. Sin embargo, cada vez que se navega por internet o se interactúa por redes sociales se expone información que puede ser usada maliciosamente por personas con habilidades técnicas en seguridad informática, llamados “hackers”, y podemos ser víctimas de ciberataques.

Generalmente los **ciberataques** comprenden un propósito delictivo como robo de dinero y/o usurpación de identidad y, ante este escenario, Freddy Alvarado, especialista en ciberseguridad y privacidad de **ESAN Graduate School of Business,** brinda cinco consejos para que evite caer en fraude digital.

1. Usa una red confiable

Muchas veces las personas se conectan a redes de wifi públicas, desde centros comerciales o aeropuertos, y es a través de estas redes poco seguras que a los **hackers** se les facilita el acceso a los dispositivos para realizar ilícitos. Si se va a llevar a cabo una transacción bancaria, acceda a una conexión segura. Las empresas utilizan la red VPN; es decir, una red privada donde se aíslan intentos de ataque.

2. Accede a enlaces originales y compruebe la seguridad

Para evitar ciberataques no navegue en aquellos enlaces que provienen de un correo sospechoso. En el caso de un navegador Chrome, puede verificar la **seguridad del sitio** dirigiéndose a la izquierda de la dirección web.

Si aparece un candado plomo, es seguro; si es un signo de exclamación en un círculo, el lugar no usa una conexión privada; y si figura uno de exclamación enmarcado de un triángulo rojo, significa que el sitio es peligroso.

3. Maneja claves fortalecidas

No use la misma clave para las principales cuentas. Las contraseñas son una importante **barrera de seguridad** y deben ser fortalecidas con diferentes criterios.

Agregue signos o caracteres como “@”, “#” u otros símbolos, e intercale entre minúsculas y mayúsculas. Además, no repita las contraseñas en los accesos principales de redes sociales, bancos u otro tipo de cuentas personales y es recomendable cambiarlas cada tres meses.

4. Opta por múltiples opciones de validación en cuentas virtuales

Muchas cuentas de redes sociales e internet permiten una

verificación mediante huellas dactilares, aprobación directa al celular, mensajes de texto o códigos dictados por llamada. Se recomienda que confíe siempre su información en sitios que ofrecen múltiples opciones de validación para accesos.

5. Instala un antivirus en todos sus dispositivos

Para la identificación de los software maliciosos de los hackers, los antivirus realizan un análisis continuo de los archivos. Se comparan con características particulares de distintos ejemplares de “malware” encontrados con anterioridad, indicó **Freddy Alvarado de ESAN**.

Estos programas se pueden instalar en computadoras de escritorio, laptops, tablets y celulares, y lo defienden de “gusanos informáticos”, “troyanos” y “virus”, entre otros.