MANUAL DE SEGURIDAD PARA CLEINTES

Documento elaborado el 14/02/2024

INTRODUCCIÓN

EMPROTEL S.AS fiel a la política de protección de los clientes y la generación de experiencias que trasciendan ha diseñado esta breve guía sobre protección en la red y las comunicaciones mediadas por aparatos tecnológicos, recomendamos a todos/as nuestros/as clientes seguir las sugerencias y adoptar medidas de seguridad en la red.

DEFINICIÓN

"La **seguridad informática**, también conocida como **ciberseguridad**,[1] es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.[2] Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La ciberseguridad comprende *software* (bases de datos, metadatos, archivos), *hardware*, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», esta última solamente se encarga de la seguridad en el medio informático, pero por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos.

La seguridad de la información nos habla sobre métodos y procesos que procuran proteger los archivos de información en sus diferentes formas y estados, mientras que la seguridad informática nos habla sobre métodos y procesos técnicos para la protección de la confidencialidad, disponibilidad e integridad de la información.

La seguridad informática también se refiere a la práctica de prevenir los ataques maliciosos, a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos, etc."[1]

RECOMENDACIONES

Basados en múltiples evidencias de violentación de la privacidad y conscientes e la vulnerabilidad de la mayoría de los usuarios de internet, y con el fin de prevenirles de fraudes, estafas, engaños, robo de información sensible, suplantación de identidad, recomendamos:

Usuarios y Contraseñas

- Use contraseñas robustas, haga una fusión entre letras, números y caracteres especiales, incluya letras mayúsculas y minúsculas, evite fechas de cumpleaños, aniversarios, nacimientos, números de cédula, no las porte escritas en su billetera o en el teléfono, mucho menos en agendas o cuadernos de fácil acceso.

[1] Tomado de: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

- No comparta por ningún medio los usuarios ni contraseñas de sus sitios importantes, mucho menos comparta imágenes que contengan esta información.
- Cambie las contraseñas con cierta periodicidad, mantenga un patrón que usted pueda recordar con facilidad sin recurrir a anotarlas y portarlas.
- Que la longitud mínima de sus contraseñas sea de 6 caracteres.

Conexiones en Redes Públicas

- Tenga mucho cuidado cuando accede a Redes Públicas (WIFI Gratuito), a veces por ahorrarnos unos megas terminamos entregando información sensible.
- No predefina las redes en sus dispositivos, o sea no las guarde de manera permanente.
- No predefina los métodos de acceso en esas redes públicas.
- No comparta información sensible a través de redes públicas, información que contengan claves, usuarios, códigos secretos, respuestas a pregunta claves.
- Nota: Puede usarlas las veces que quiera, pero tome las medidas pertinentes

Respuestas a Mensajes vía E-mail o mensajería

- Evite responder correos electrónicos de personas desconocidas o que aparezcan en su bandeja de entrada con origen sospechoso o no solicitado por usted o que se encuentren en la bandeja de correos no deseados o spam, muchas ocasiones estos comunicados alojan enlaces que vulneran su seguridad informática a través de diferentes mecanismos, otras ocasiones tienen títulos o asuntos llamativos como: *"te comparto las fotos del viaje", "felicitaciones eres ganador", "quiero hacerte una donación", "participa en el sorteo",* etc., este y otros títulos tentadores pueden hacerte caer en la trampa, para evitarlos recuerda**: ¡Lo barato sale caro!**
- Evite responder correos que contienen publicidad, no hace falta, aunque vengan de destinatarios seguros o conocidos, muchas ocasiones los estafadores buscan enmascarar su delito en marcas reconocidas, recuerda **¡Desconfiar es lo más confiable!**
- Por nada del mundo compartas cadenas y mucho menos abras sus enlaces.
- No respondas ni des clic en mensajes SMS, Messenger o wapp que te llegan indicando que "tu paquete ya llegó, completa la información para que puedas retirarlo"

Navegación de niños/as

Para empezar, nunca predefinas formas de pago o cargues datos de tu tarjeta de crédito o débito para pagos automáticos, la inexperiencia de los niños te va a pasar una enorme factura, bloquea todo lo que puedas, de preferencia no les des tus dispositivos los/as niños/as para que jueguen libremente, pero si crees que es un mal consejo, sigue estas sugerencias:

- Establece franjas horarias de navegación.
- Bloquea aplicaciones que contengan información bancaria, crediticia y otra sensible.
- Controla las aplicaciones a las que acceden tus hijos, los delincuentes de la red los manipula, incluso -off line- para que les compartan datos sensibles o para inducirles a prácticas y conductas inapropiadas.
- Ten cuidado con los juegos, aparentemente son inofensivos, pero detrás de estos hay depravados y estafadores, por si fuera poco, estos sitios están infestados de virus.
- Mucho ojo con los contenidos para adultos, además de depositar virus en tus equipos, es probable que te veas tentado a facilitar datos que no debes.

Recomendaciones finales

Antes de dar clic en un enlace o de responder un mensaje o de abrir una página, hazte estas preguntas:

- ¿Lo solicité?
- ¿Lo esperaba?
- ¿Los conozco?
- ¿Se de qué me hablan o me ofrecen?, y si tienes dudas, especialmente en servicios bancarios, crediticios, internet, paquetería, compras; **llama al call center oficial** de tu proveedor, así despejas dudas y mejor aprovechas para conocer de mano alguna oferta importante que sí te beneficie

Con este simple ejercicio estarás un poco más a salvo.

- **FIN DEL DOCUMENTO**: Instruir a los/as usuarios/as sobre los derechos enmarcados en la Ley de Protección de datos
- **ELABORADO POR**: Equipo Técnico EMPROTEL S.A.S, para NAUTA Servicios de Internet.
- **FECHA DE ELABORACIÓN**: 14/02/2024
- **FUENTE**: Ley Orgánica de Protección de Datos.