RECOMENDACIONES BÁSICAS PARA USUARIOS FINALES

De acuerdo al crecimiento del ciberdelito, especialmente el ataque conocido como RASOMWARE (encripta la información dejándola inaccesible), es importante conocer que no existen medidas de seguridad o protección informática absoluta, sobre todo mientras trabajemos en red o conectados a internet. Por lo tanto, es importante tomar recaudos y acciones para mitigar el riesgo de recibir un ataque de esta naturaleza y en el caso de sufrirlo estar preparados para la recuperación, restauración y normalización de la actividad. Las fuentes de ingreso de ataques RASOMWARE más comunes son: archivos infectados recibidos por correo electrónico, links publicitarios engañosos que al acceder infectan nuestra computadora.

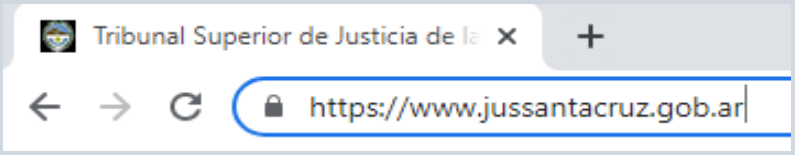
Hemos recopilado estas sencillas recomendaciones básicas de seguridad informática, para que su sistema, información y datos se mantengan libres de infecciones. Si los pone en práctica, las posibilidades de contagio serán considerablemente menores.

NAVEGAR EN LA WEB DE FORMA SEGURA

Siempre es recomendable navegar por páginas web seguras y de confianza. Para diferenciarlas del resto, identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Las páginas que tienen seguridad en su acceso se pueden identificar de las siguientes dos maneras:

La dirección de la página debe comenzar con el prefijo https:// en lugar de http://.

En la barra del navegador debe aparecer el icono del candado cerrado. Haciendo clic en este icono se puede acceder al certificado digital que confirmarla autenticidad de la página.



Ambos elementos le garantizan que los datos e información que comparta en esa página están cifrados y no se pueden interceptar.

Evite navegar por páginas dudosas y responder los carteles de seguridad o de advertencia que aparecen al navegar en sitios o páginas desconocidas. Siempre lea el mensaje y ante la mínima duda, evite hacer clic alguno en el cartel y cierre el navegador o la/s pestaña/s del mismo afectadas.

LINKS DUDOSOS

No acceder a links de publicidades engañosas.

ATENCIÓN CON LOS CORREOS ELECTRÓNICOS

Caer en engaños como el phishing (Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios) puede ser muy fácil si no revisa los ***e-mails*** con detenimiento. Asegúrese de conocer al remitente, fíjese si la dirección o el mensaje están escritos correctamente. **Si cree que no es un correo seguro**, **no abra los archivos adjuntos** (por ejemplo, fotos, pdf, documentos) ni responda, directamente elimínelo. Y ¡nunca comparta información sensible!

CAMBIE SUS CONTRASEÑAS CON REGULARIDAD

Para prevenir que terceros accedan a su información, le recomendamos actualizar sus contraseñas por lo menos 4 veces al año y evitar el uso de la misma clave en todas sus cuentas. No olvide crear contraseñas seguras, complejas, pero, a la vez, de fácil recordación.

REALICE COPIAS DE SEGURIDAD DE SUS ARCHIVOS PERSONALES

Si un hacker accede a su información, la modifica o la elimina, tener un respaldo o copia de seguridad le ayudará a recuperar sus datos y quedarse tranquilo. Actualmente, puede hacerlas en la nube para casi todos sus dispositivos. Otra alternativa es guardar un respaldo por ejemplo en un pendrive. Nosotros realizamos periódicos respaldos de servidores y datos, pero no los de uso personal.

MANTENER ACTUALIZADO EL SOFTWARE DE SUS DISPOSITIVOS PERSONALES

Las nuevas versiones de software tienen parches de seguridad que refuerzan los puntos vulnerables por donde los hackers pueden acceder a su computadora o celular.

Le recomendamos configurar automáticamente todas las actualizaciones de sus dispositivos personales.

CERRAR SESIONES DE TRABAJO Y CUENTAS

Al finalizar el uso, tanto de Lex Doctor, correo electrónico, etc. cerrar las correspondientes ventanas.

CUIDADO CON LA REDES PÚBLICAS O EXTERNAS

Las redes públicas de internet no cifran la información que circula a través de ellas; por eso, sus datos no están protegidos cuando las usa. Lo ideal es que no efectúe transacciones o gestione información sensible desde un WIFI público.

UTILIZAR ANTIVIRUS EN EL ORDENADOR

Cada día obtenemos mayor información externa, descargamos ficheros y navegamos mucho por internet. Por lo tanto, es esencial que el ordenador tenga un antivirus instalado y actualizado que revise posibles amenazas.

DIRECCIÓN DE INFORMÁTICA

PLUSNET INTERNET

WEBGRAFÍA

www.jussantacruz.gob.ar
https://www.incibe.es/
CSA (cloudsecurityalliance.org)
www.redbooks.ibm.com