Recomendaciones de Ciberseguridad

Como se ha visto en los últimos días, el país ha sido víctima de diferentes ataques informáticos que han afectado la integridad de los datos y se han visto interrumpidos los servicios que se brindan por medio de los sistemas de la información.

Los ataques recibidos por diferentes instituciones están relacionados principalmente con el ransomware denominado “Conti”, el cual es un software malicioso que generalmente se recibe mediante archivos adjuntos en correos electrónicos, y encripta los datos de las computadoras imposibilitando el acceso a la información. Las actividades maliciosas asociadas al software denominado malware, incluyendo el ransomware es un tipo de ataque informático que tiene la capacidad de replicarse una vez que ha sido descargado y restringe el acceso al sistema operativo infectado, secuestrando los datos de las personas usuarias para posteriormente solicitar un pago de rescate, que no siempre asegura la recuperación de la información.

Por lo tanto se hace necesario estar atentos para no ser victimas de estos ataques informáticos, por lo cual se extienden las siguientes recomendaciones y puntos importantes a tomar en cuenta, para evitar un ataque informático.

1. **Actualizaciones de software**: se debe tener siempre actualizados los softwares de nuestra computadora, celulares y otros equipos tecnológicos que utilicemos. Por lo cual se debe revisar lo siguiente:
    a. En el caso de las computadoras se debe revisar diariamente que no se encuentren actualizaciones de Windows pendientes de instalación, en caso contrario se deben aplicar las actualizaciones correspondientes. En el siguiente enlace se puede visualizar un manual para verificar y actualizar Windows: http://www.etcg.una.ac.cr/index.php/documento-electronico/category/53-seguridad-informatica?download=284:manual-actualizacion-de-windows
    b. En el caso los celulares o otros dispositivos inteligentes, se debe estar atento a las actualizaciones de sistemas operativo y de las aplicaciones para que siempre se tenga la ultima versión disponible. En el siguiente enlace se puede visualizar el manual para verificar y actualizar los sistemas operativos de los dispositivos y aplicaciones móviles: http://www.etcg.una.ac.cr/index.php/documento-

electronico/category/53-seguridad-informatica?download=285:manual-actualizacion-dispositivos-moviles

2. **Respaldo de la información:** Se debe respaldar la información importante periódicamente en un dispositivo externo tipo llave USB o Disco duro externo, para que en el caso de recibir un ataque, poder recuperar la información. También existe la opción de respaldo de la información en la Nube, con los servicios que ofrece la Universidad Nacional, como lo son Google Drive y OneDrive, tomando en cuenta que su capacidad es limitada. En el siguiente enlace se puede visualizar manual para respaldo de información en medios en la Nube: http://www.etcg.una.ac.cr/index.php/documento-electronico/category/53-seguridad-informatica?download=286:manual-respaldo-informacion-en-la-nube
3. **Correos electrónicos Maliciosos:** Se debe de poner especial atención a los correos electrónicos que contengan enlaces y archivos adjuntos. Se debe de verificar el remitente del correo y si se ve sospechoso consultarlos con el informático de la escuela. Además no descargar archivos adjuntos que terminen en .bat o .exe ya que estos archivos son ejecutables que pueden infectar la computadora. Por otro lado, pueden llegar correos electrónicos con formularios para que ingrese información personal sensible como nombres de usuario y contraseñas, por lo que debe evitar ingresar ese tipo de datos por medios electrónicos o por llamadas telefónicas.
4. **Sitios Web:** Siempre que se acceda a un sitio web se debe verificar que en la parte superior izquierda al lado de la dirección URL, se despliegue un icono de candado de seguridad, que refleja que se trata de un sitio seguro. También verificar que la dirección URL no se vea sospechosa o extraña. Por otro lado si se ve un cantidad excesiva de anuncios y ventanas emergentes en el sitio, lo recomendable es abandonar el sitio ya que pueden ser descargado archivos maliciosos que comprometan el equipo de cómputo. También evitar visitar sitios web desconocidos.
5. **Enlaces Maliciosos:** Cuando se navegue por redes sociales, correos electrónicos o sitios web, evitar dar clic en los enlaces o links que se despliegan, ya que pueden iniciar la descarga de algún malware o desplegar algún sitio falso, donde se pidan datos personales y contraseñas, y puede verse expuesto a un fraude bancario o hackeo de alguna de sus cuentas.

6. **Contraseñas:** Se recomienda el cambio de las contraseñas al menos dos veces al año, y con las recientes noticias, se debería hacer con una periodicidad menor. Además, las contraseñas no deben hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, nombre de usuario, meses del año, nombres de personas, teléfonos o similares. La longitud mínima de las contraseñas debe ser igual o superior a ocho (8) caracteres, se recomienda utilizar contraseñas de la mayor longitud posible, que puedan ser recordadas para evitar fraudes o vulneraciones. Las contraseñas deben estar constituidas por una combinación de letras mayúsculas, minúsculas, números o caracteres especiales. La contraseña no debe contener vocales.

Clase	Descripción de la clase
Letras Mayúscula	B,C,D... Z
Letras Minúsculas	b,c,d... z
Números	0,1,2,3... 9
Caracteres Especiales	¡!#$%&@.()

7. **Contraseña en computadoras:** Las computadoras debe tener contraseña de acceso o de inicio de sesión, si desconoce como establecer la contraseña en Windows o cambiarla, consultarlo con el informático de la escuela.
8. **Revisión de USB:** Cuando conectamos un dispositivo almacenamiento USB, tipo llave maya o Disco duro externo, el antivirus de la computadora por lo general indica que si acepta realizar la revisión del dispositivo en busca de algún virus, no se debe omitir esta revisión ya que es una medida de seguridad para poder encontrar algún virus antes de que infecte el equipo de cómputo.
9. **Configuración del Explorador de archivos:** Se debe aplicar una configuración para poder ver la extensión de los archivos de la computadora con el fin de evitar la ejecución de cualquier archivo que tenga extensión o que termine en .bat o .exe. En el siguiente enlace se puede visualizar manual para configurar la visualización de extensiones en Windows: http://www.etcg.una.ac.cr/index.php/documento-electronico/category/53-seguridad-informatica?download=287:manual-configuracion-visualizacion-extensiones

Todas las recomendaciones anteriores son importantes para evitar un posible ataque informático y cuidar la información de nuestros equipos de cómputo.

Además, si tiene sospechas de que esta ante un ataque informático en su equipo de cómputo, apague el equipo y póngase en contacto con el informático de la escuela.

Cualquier duda sobre las recomendaciones indicadas y de como aplicarlas, consúltele con el informático de la escuela.