UNIVERSIDAD DE GRANADA

Secretaría General

Decálogo de Ciberseguridad

Con motivo del Día Mundial de Internet, la Universidad de Granada ha preparado un decálogo de buenas prácticas de ciberseguridad. Conocer dichas prácticas e integrarlas en nuestros hábitos relativos al uso de la tecnología nos permitirá un uso más seguro de la misma tanto en el ámbito personal como laboral.

Para aquellos miembros de la comunidad que quieran ampliar la información o resolver dudas, pueden dirigirse a la Centro de Atención al usuario a través de la dirección @email.

Se puede descargar la infografía del decálogo con un resumen de las recomendaciones aquí detalladas para tenerlas siempre a mano

- **1.- Gestiona tus contraseñas**

  Las contraseñas son un mecanismo básico que nos permite identificarnos en un servicio, por tanto, deben ser seguras para evitar ser suplantados. Básicamente dos formas de dificultar el que un atacante pueda adivinarlas, o romperlas, sería cambiarlas con cierta frecuencia (especialmente cuando se sospecha que ha podido ser descubierta) o hacerlas fuertes de forma que el tiempo que necesita un atacante para obtenerla sea elevado.

  Dos factores importantes para construir una contraseña fuerte: la complejidad (poco predecible) y la longitud, teniendo en cuenta que prima la longitud. Por tanto debemos construirlas como una cadena de caracteres que contenga números, letras (mayúsculas y minúsculas) y signos especiales con al menos de 8 caracteres de longitud (adecuados sin se usa con doble factor de autenticación), pero como a mayor longitud más fortaleza, tendremos una clave más fuerte a partir de 12 caracteres como recomiendan las guías de buenas prácticas más recientes.

  Además, dicha cadena debería tener una longitud mínima de 8 caracteres para que el tiempo para romperla lo haga inviable. Si bien esta dos guías de formación pueden hacernos pensar que serían muy difíciles de memorizar por el usuario, existen reglas de formación que permiten generar una contraseña suficientemente larga y compleja fácil de recordar y difícil de romper/adivinar. Algunas reglas son:

  - Utilizar la concatenación de varias palabras para construir contraseñas largas cuya deducción, automática o no, no sea simple.

- Las contraseñas no deberán estar compuestas de datos propios que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, etc.), ni ser frases famosas o refranes, ni ser estrofas de canciones o frases impactantes de películas o de obras de literatura.
- La contraseña así formada no deberá ser igual a ninguna de las últimas contraseñas usadas, ni estar formada por una concatenación de ellas.
- Las contraseñas deberán sustituirse por otras si existe evidencia de que hubieren sido comprometidas.

Diferentes en cada plataforma: no debemos usar la misma contraseña en diferentes plataformas o servicios. Tampoco deben basarse en un patrón dependiente de la plataforma ya que es fácil adivinarlo por un atacante.

Gestores de contraseñas: Dado que actualmente debemos mantener un número elevado de contraseñas, lo más cómodo y seguro es usar un gestor de contraseñas. Esta aplicación nos permite almacenar en una base de datos cifrada tomas las contraseñas y solo necesitamos memorizar una contraseña maestra para acceder a dicha base de datos. Además, nos permite asignar/generar contraseñas muy fuertes al no tener que memorizarlas. También es recomendable activar el doble factor de autenticación en aquellos servicios que lo permitan, como cuentas de redes sociales.

Debemos evitar almacenar las contraseñas directamente en el navegador, ya que si bien es cómodo, estas no están suficientemente protegidas cuando navegamos. De tener que hacerlo, sería conveniente usar el gestor de contraseñas embebido en el navegador ya que dificulta en acceso a las mismas por terceros.

Para finalizar, recordar que no se debe compartir la clave con nadie, ni enviar por ningún medio (correo, SMS, etc.) y, por supuesto, añorarlos en un soporte no protegido de forma segura.

- **2.- Usa antivirus**

  El uso de alguna de las aplicaciones actuales para la detección del malware (antivirus) nos defenderá frente a un elevado número de aplicaciones maliciosas que intenta infectar nuestros equipos. Además, los antivirus actuales incorporan nuevas características de seguridad de nuestros equipos y la información que almacenan.

  Para una mayor protección debemos usar aquellos antivirus que actualicen regularmente la base de datos de muestras.

  Estas herramientas se complementan con el punto 10 de decálogo “Navegación segura” para alcanzar una mayor protección.

  Deberíamos instalar un programa antivirus en todos los equipos que usemos. Pese a lo que podemos creer, los antivirus actuales no consumen una cantidad apreciable de recursos.

- **3.- No dejes tus dispositivos desatendidos**

No debemos pensar que los ataques a los sistemas siempre proceden del exterior. Cada vez con más frecuencia encontramos ataques donde participa alguien que tiene acceso físico a nuestros sistemas, por lo que es básico proteger el acceso a los mismos.

En este sentido, una medida muy sencilla de implementar el bloqueo de la sesión de trabajo o la pantalla de nuestro equipo (sea de forma automática o manual) cuando nos ausentamos del puesto, aunque sea por un corto periodo de tiempo. Este simple acto evitará el acceso de personas no autorizadas tanto a la información como al uso del dispositivo.

- **4.- Haz copias de seguridad**

  No solo debido a un incidente de seguridad, sino a un malfuncionamiento del hardware/software o a un error humano, pueden provocar que perdamos la información almacenada en nuestro equipo.

  Dado que nos puede pasar en cualquier momento un medida básica es la de realizar copias de seguridad regularmente. Actualmente hay numerosas aplicaciones para realizarlas de forma automática, incluidas en algunos sistemas en el propio sistema operativo.

  El coste de un sistema para las copias de seguridad, ya sea bien en la nube o en soportes externos no es muy elevado y, en cualquier caso, esta inversión se ve rentabilizada con creces antes muchos tipos de incidentes que podemos sufrir. Ahora bien, sea cual sea la solución, el sistema de respaldo debe esta desconectado de nuestro equipo cuando la copia de seguridad no esté en marcha.

- **5.- Mantén actualizados tu sistema operativo y las aplicaciones.**

  Una fuente importante de amenazas para nuestros equipos son las vulnerabilidades que pueden presentar tanto el hardware como el software. Estas permiten que un atacante las explote y tenga acceso a nuestros sistemas.

  Los fabricantes de hardware/software están constantemente corrigiendo dichas vulnerabilidades y publicando las nuevas versiones corregidas para que los usuarios puedan actualizar sus sistemas de cara a alcanzar una mayor protección. Por ello, siempre que sea posible es importante actualizar a la mayor brevedad tanto el sistema operativo como las aplicaciones que tenemos instaladas, especialmente los navegadores y sus extensiones. La mayoría de las aplicaciones disponen de una opción de actualización automática que solo debemos activar.

- **6.- Aplicaciones seguras**

  La instalación de aplicaciones de fuentes no confiables puede provocar problemas de seguridad como instalación de programas maliciosos o filtración de datos, entre otros. También problemas relacionados con un funcionamiento incorrecto el sistema.

Por tanto, se deben descargar desde sitios oficiales ya sean para equipos de sobremesa como móviles. En este último caso, también dudar de aquellas aplicaciones que soliciten permisos excesivos o innecesarios para la funcionalidad requerida.

- **7.- Usa cifrado de datos**

  Los dispositivos de almacenamiento y especialmente los extraíbles, como pendrives, son susceptibles de pérdida o robo. Si le unimos que pueden contener información personal o sujeta al reglamento de protección de datos, debemos cerciorarnos de que quién los encuentre no tenga acceso a dicha información mediante el cifrado bien de la unidad completa bien de los archivos sensibles contenidos en ella. Este cifrado se puede realizar con herramientas incluidas en el propio sistema operativo o aplicaciones de terceros.

- **8.- Cuidado con el phishing**

  Los ataques de phishing son un tipo de técnica que usan la ingeniería social destinada a obtener fraudulentamente información personal de los usuarios, o que el receptor del mensaje instale malware en lugar de hacerlo el atacante, mediante correos electrónicos que aparentan ser fiables para recabar datos de carácter personal (cuentas bancarias, credenciales, etc.), derivar en páginas web falsas o que ejecutemos un archivo adjunto. Aunque el correo es la vía más conocida también se pueden utilizar SMS (smishing) o por teléfono (vishing).

  Aspectos que debemos fijarnos en el caso de recibir un correo electrónico no solicitado:

  - Solicita información sensible (personal, pagos, etc.) o solicita alguna acción cuyo procedimiento no es la norma y no ha sido solicitada por parte del receptor.
  - Tiene inconsistencias entre la dirección de correo, los enlaces o los nombres de dominio.
  - Incluye adjuntos no solicitados y trata de que pinchemos en ellos.
  - No esta personalizado.
  - Esta mal redactado, tiene faltas de ortografía o utiliza un saludo desconocido
  - Aborda temas que llaman nuestra atención y solicita respuesta urgente.

  Estos correos fraudulentos son relativamente frecuentes y debemos aprender a identificarlos ya que son una de las principales amenazas de seguridad. Puedes consultar más información en la página de Andalucía Vuela o en la de INCIBE.

- **9.- Minimiza tu huella digital**

Debemos tener presente que cualquiera de nosotros puede ser víctima de un ciberataque. Los atacantes pueden utilizar la información disponible en Internet sobre nosotros, nuestra huella digital, para materializar un ataque. Por ello, es importante minimizar al máximo la información personal que publicamos en Internet, especialmente en las redes sociales.

Para borrar dicha información de la red podemos ejercitar el derecho que suministran diferentes plataformas, tal como se recoge en la página de Andalucía Vuela.

En este sentido es conveniente no registrar servicios externos a nuestra universidad usando las cuentas de correo institucionales ya que dichas cuentas pudieran verse comprometidas.

- **10.- Navega de forma segura**

  El acceso a sitios web no seguros puede comprometer nuestros equipos (ataques, fraudes, estafas, robo, etc.) y nuestra privacidad, por tanto, es muy importante reconocer dichos sitios.

  Algunos de los elementos que debemos considerar para identificar la confianza en un sitio web son:

  - Mirar en la barra de direcciones web que la dirección a la que deseamos acceder comienza por https, que nos garantiza que nuestros datos viajan seguros.
  - Mirar que la dirección esta bien escrita, ya que en ocasiones los atacantes usan sitios web falsos con direcciones parecidas a la del sitio que quieren suplantar.
  - En la barra de direcciones y delante de la dirección, debe aparecer un candado cerrado que garantiza que el servidor posee un certificado digital que garantiza la seguridad del sitio y cuyos datos pueden ser verificados.
  - Evitar sitios que tenga publicidad agresiva o ventanas emergentes que aparecen de forma insistente, especialmente cuando solicitan información personal.
  - Fijarnos en que tengan definida la política de privacidad y aparezcan los datos del propietario del sitio para poder cotejarlos.
  - Debemos tener cuidado cuando se produzcan redireccionamientos, es decir, cuando el sitio web nos reenvía a otra dirección, en cuyo caso hay que analizar el nuevo sitio.
  - Especial atención debemos tener con las direcciones acortadas ya que no sabemos a qué sitio nos llevan.
  - Con especial interés en la privacidad, debemos leer atentamente la política de cookies (archivos que intercambian los servidores web con nuestro navegador) del sitio, y en caso de que sea necesario, los navegadores poseen los mecanismos para borrar dichas cookies cuando no sean necesarias. Se puede valorar el uso de extensiones del navegador para bloquear la publicidad o evitar ser rastreados.

Afortunadamente este proceso se va simplificando ya que con mayor frecuencia los motores de búsqueda o los propios navegadores incorporan mecanismo para determinar la confianza de un sitio y ajustar nuestras propias opciones de seguridad y privacidad. Además, tenemos herramientas que permiten verificar el sitio antes de que accedamos y, en caso de que no sea seguro, nos muestran una advertencia. Algunos antivirus proporcionan esta funcionalidad, pero si no podemos comprobarlo nosotros mismos con páginas como la de VirusTotal, donde con solo escribir la dirección nos indicará si es, o no, maliciosa.

Una relación detallada de buenas prácticas de navegación web podemos encontrarla esta guía del CCN y las relacionadas con privacidad en la guía de la AEPD y las OSI.