SEGURIDAD DIGITAL EN CONSERVATORIOS: MANUAL DE AYUDA PARA DOCENTES

1. Privacidad y seguridad en internet

La situación que estamos viviendo a causa de la pandemia del COVID-19 ha afectado a muchísimos sectores, entre ellos el de la educación. Hemos tenido que cambiar nuestros hábitos y costumbres y adaptarnos a una normalidad que nunca hubiéramos imaginado: la de dar clases a distancia. A raíz de estos cambios nos han surgido muchas preguntas, algunas de ellas relacionadas con la seguridad en internet. Por eso hemos pensado que es un buen momento para proporcionar algunos consejos para docentes e intentar resolver algunas dudas sobre ciberseguridad.

Como profesores tenemos que tomar conciencia del entorno en que nos movemos cotidianamente, teniendo en cuenta, por supuesto, nuestro ámbito docente. Vivimos en una sociedad en la que está siempre presente un tipo de ambiente digital, colaborativo y conectado a internet.

En este tipo de entorno colaborativo, en el que creemos que aparentemente todo son ventajas, debemos aprender que no estamos exentos de amenazas.

Pese a todas las dificultades que nos hemos encontrado, esta situación ha abierto también una ventana para que los centros docentes afronten nuevas oportunidades y retos necesarios de renovación tecnológica y excelencia docente al alcance de toda la comunidad.

Son muchos los conservatorios de música que necesitan renovarse y fomentar diferentes iniciativas. Entre ellas, la de mejorar y adaptar sus infraestructuras telemáticas, buscando el equilibrio entre las clases en formato presencial y online, sin por ello alterar la calidad de la enseñanza y el aprendizaje.

Claro está que los ciberdelincuentes también ven en todo ello un sinfín de oportunidades para poder llevar a cabo sus acciones delictivas y fraudulentas. No hay que bajar la guardia. Es y seguirá siendo fundamental dedicar esfuerzos y recursos para elaborar e implementar planes de formación que mejoren el grado de concienciación de todos los usuarios y agentes implicados.

1.1. ¿Qué es la ciberseguridad?

Aunque el concepto de ciberseguridad parece que fuera preocupación únicamente de los informáticos o ingenieros, lo cierto es que es un tema que atañe a cualquier persona que utilice algún dispositivo conectado a la Red.

Pero ¿a qué nos referimos cuando hablamos de ciberseguridad? Esto es, la práctica de defender y proteger tanto los dispositivos y sistemas electrónicos como a los servidores que los soportan de posibles peligros y ataques maliciosos.

1.2. Objetivos

- Tratar las medidas primordiales de protección de los dispositivos digitales al alcance de todo el profesorado.
- Saber la manera de eludir virus, evitando también los fraudes y la desinformación que circula vía digital.
- Informar a la comunidad educativa, en lo referente a la protección de la privacidad y reputación online.

2. Uso saludable de Internet

Debemos ser conscientes, en todo momento, de los riesgos a los que nos estamos enfrentando cuando nos conectamos a internet. Nos referimos entre otros a los virus, fraudes, y en general a todo tipo de desinformación en la red.

La ingeniería social, puede ser utilizada por los ciberdelincuentes, manipulando a los usuarios de internet, con el fin de conseguir información personal, o para obtener acceso a los equipos personales.

2.1. Seguridad y buenas prácticas

Ante todo, recordemos que internet está formada por redes de millones de ordenadores conectados entre sí y que la información, una vez subida a internet, ya nunca desaparece. Siempre queda rastro en algún rincón recóndito de internet sin que nosotros lo sepamos. Así pues, lo más recomendable es publicar siempre información que en ningún caso pueda comprometernos.

Además, es importante adoptar una serie de buenas prácticas para proteger el acceso y la salvaguarda de nuestra información. Por ejemplo:

- Utilización de antivirus en todos los dispositivos que utilicemos.
- Implementar una política de contraseñas adecuada.
- Realizar copias de todo el contenido que generamos, tanto en la nube (online) como en un disco duro externo (offline).
- Utilizar el email laboral en vez del email personal.
- Fomentar el uso de herramientas seguras.
- Verificar los enlaces antes de pulsar en ellos.
- Nunca descargar ficheros adjuntos que sean sospechosos.

3. Plan estratégico educativo de seguridad y privacidad en la red

El robo o suplantación de identidad es uno de los objetivos más comunes en la mayoría de los ciberataques. Permite al agresor hacerse pasar por la víctima y, por ende, acceder a sus aplicaciones e información confidencial o financiera.

3.1. Riesgos y propuestas ante incidentes

La forma más frecuente de conseguir dicha información es a través de ataques de phishing que gozan de una gran probabilidad de éxito. Utilizan técnicas basadas en ingeniería social y se fundamentan en el engaño. La mejor práctica para evitar el robo de cuentas y la suplantación de identidades es entender que debemos evitar publicar y nunca debemos facilitar por teléfono, mensaje de texto o correo electrónico:

- Nuestro correo electrónico, para no estar implicados en campañas de Phishing.
- Nuestro número de teléfono para no estar sometidos a campañas de Smishing.
- Nuestra dirección y ubicación, evitando así persecuciones, ataques físicos e incluso robos.
- Información personal como contraseñas y documentos personales como el DNI.
- Información bancaria, como números de cuenta y tarjetas bancarias.
- Fotografías y vídeos de otras personas sin contar con su consentimiento.
- Fotografías personales.
- Conversaciones o videos privados.
- Opiniones, quejas o comentarios que nos puedan comprometer, ya que desde el primer segundo que lo publicamos, perdemos el control inmediatamente sobre lo publicado.

Además, también es recomendable preguntar al emisor del mensaje por la información que tiene sobre nosotros. Si no la sabe, empecemos a dudar.

Las cámaras conectadas en todo momento son por definición una mala práctica ya que almacenan información (pudiendo grabar información sensible) que tal vez no deseemos compartir. Es aconsejable utilizar “cubiertas” en las webcams de los ordenadores que abrimos manualmente sólo cuando las vayamos a usar (por ejemplo, al realizar una videollamada o una reunión telemática).

3.2. Técnicas eficientes

Reiteramos que lo más importante es entender y asimilar que el eslabón más débil en la cadena de ciberseguridad es el ser humano. Por lo tanto, la mejor

defensa empieza por educar y concienciar al profesorado sobre los peligros de la red.

Los mecanismos básicos de defensa ante este tipo de ataque serían:

- No precipitarse nunca en aportar información (piensa, luego actúa).
- Indagar y preguntar al interlocutor sobre la información que tiene de nosotros.
- En ningún caso, facilitar información personal relacionada con nuestras cuentas bancarias ni con nuestras contraseñas.

Y, en resumen, los fundamentos básicos para gestionar adecuadamente nuestra información serían:

- Utilizar contraseñas fuertes y seguras para acceder a nuestras aplicaciones que combinen una serie de unos 8-12 caracteres aleatorios de letras mayúsculas, minúsculas y números.
- Utilizar "cubiertas" en las cámaras (webcams) de nuestros ordenadores.
- Hacer copias semanales de la información que vamos generando (almacenadas en la nube).
- Impedir que terceros accedan a nuestros dispositivos electrónicos. Tener cuidado con los dispositivos compartidos.
- Comprobar si el sistema de nuestros dispositivos está protegido. Utilizar antivirus en todos los dispositivos, en particular en los móviles, en los que utilizamos plataformas y aplicaciones del centro educativo.
- Realizar copias de seguridad.
- Comprobar los sitios a los que se accede, realizando una lista blanca de aplicaciones y páginas web.
- Buscar información en ciberseguridad en páginas de entidades cualificadas como, por ejemplo,
    - https://www.is4k.es
    - https://www.osi.es
    - https://www.tudecideseninternet.es/aepd
- Asistir a ponencias-charlas sobre ciberseguridad por entidades cualificadas (por ejemplo, del INCIBE) para estar en permanente actualización.

- Llamar ante cualquier incidente al número de teléfono 017, donde nos pueden aconsejar e informar; teléfono de ayuda en ciberseguridad que el Gobierno pone en marcha a través del Instituto Nacional de Ciberseguridad (INCIBE).