Prácticas de seguridad para artistas

La seguridad es responsabilidad de todos los profesionales de la industria.

Seguridad física

Niega cualquier acceso no autorizado a las instalaciones, así como a los equipos. Protege al personal y al equipo de cualquier peligro y daños.

- **Únicamente invita a visitantes autorizados por tu empleador.**
- **Nunca compartas tu tarjeta de acceso, llaves electrónicas o cualquier otro tipo de llave con otras personas.**
- **Mantén cualquier artículo importante, como guiones, props y dispositivos de almacenamiento guardados bajo llave cuándo no estén en uso.**

Seguridad en las contraseñas

Minimiza el riesgo de accesos no autorizados a tus cuentas.

- **Nunca compartas tu contraseña o permitas que alguien más utilice tu cuenta, tú eres responsable por toda la actividad realizada con tu clave de usuario.**
- **Periódicamente cambia tus contraseñas y siempre usa contraseñas seguras para todas tus cuentas.**
- **Usa contraseñas diferentes para los accesos de contenidos y otra para acceso a servicios.**
- **Nunca mandes información de acceso y contraseñas juntas, comparte esta información a través de dos canales separados, ej. Manda por email el usuario y la contraseña por mensaje de texto.**
- **Mantén las contraseñas seguras, nunca a la vista. (ej. Un Post-It sobre una computadora, laptop o en un disco duro encriptado).**

Seguridad del contenido

Minimiza el riesgo a accesos no autorizados a tus cuentas.

- **Sólo transfiere contenido digital por los medios seguros aprobados por tu cliente o de tu lugar de trabajo, nunca por email o servicios no encriptados cómo FTP.**
- **Tu lugar de trabajo tiene una red segura, y es tu responsabilidad mantenerla así, no conectes ningún hardware no autorizado o instales software sin permiso.**
- **Almacena el contenido digital en lugares apropiados para asegurar que esté respaldado regularmente.**
- **Solamente usa servicios de almacenamientos en la nube que sean seguros, como Google Drive o Dropbox. Esto si se tiene permiso explícito de parte del cliente o de tu empleador para hacerlo.**

Cuidados de las Redes Sociales

Manipular a los individuos para que involuntariamente divulguen información es una práctica bastante común.

- **Siempre asegúrate de leer y seguir las políticas de seguridad dadas por tu cliente y/o empleador. Nunca compartas contenido con gente que no esté aprobada por el dueño del material, tanto para recibirlo, manipularlo o verlo. Solo el equipo que esté trabajando directamente en el proyecto debe de tener acceso al contenido.**
- **Perfiles profesionales, como LinkedIn y IMDB, nunca deben de contener información de los proyectos en los que estés trabajando y que no han sido estrenados, al menos que tengas la aprobación para hacerlo.**
- **Cuándo sea posible, siempre refiérete a los proyectos usando nombres clave en lugar de usar sus títulos reales.**
- **Cuándo hables con colegas sobre trabajo en lugares públicos debes hacerlo con mucho cuidado y nunca bajo escucha de alguien que no trabaje directamente contigo.**

Accidentes de seguridad

¿Qué pasa si sospechas de una ruptura en la seguridad?

- **Cualquier sospecha de pérdida de contenido debe ser reportada inmediatamente a tu empleador o al dueño del contenido.**
- **No permitas negligencias o rupturas de seguridad hechas por otros, o "hacerse el que no ve", no reportar un incidente del que estás al tanto te hace responsable también.**
- **Cuando tengas dudas, por favor busca el consejo de tu supervisor o de tu equipo de soporte técnico.**

Ten en cuenta: Esta es una guía general escrita por el Comité de Tecnología de la VES. Las políticas específicas de seguridad pueden variar dependiendo de cada estudio, oficina o producción.

Si tienes cualquier duda o pregunta, por favor no dudes en consultar al productor, supervisor o al departamento de RH de tu empleador.

Para mayor información http://www.fightfilmtheft.org/facility-security-program.html