UAEM

REDES SOCIALES

Medidas de seguridad para proteger tu perfil

DTIC

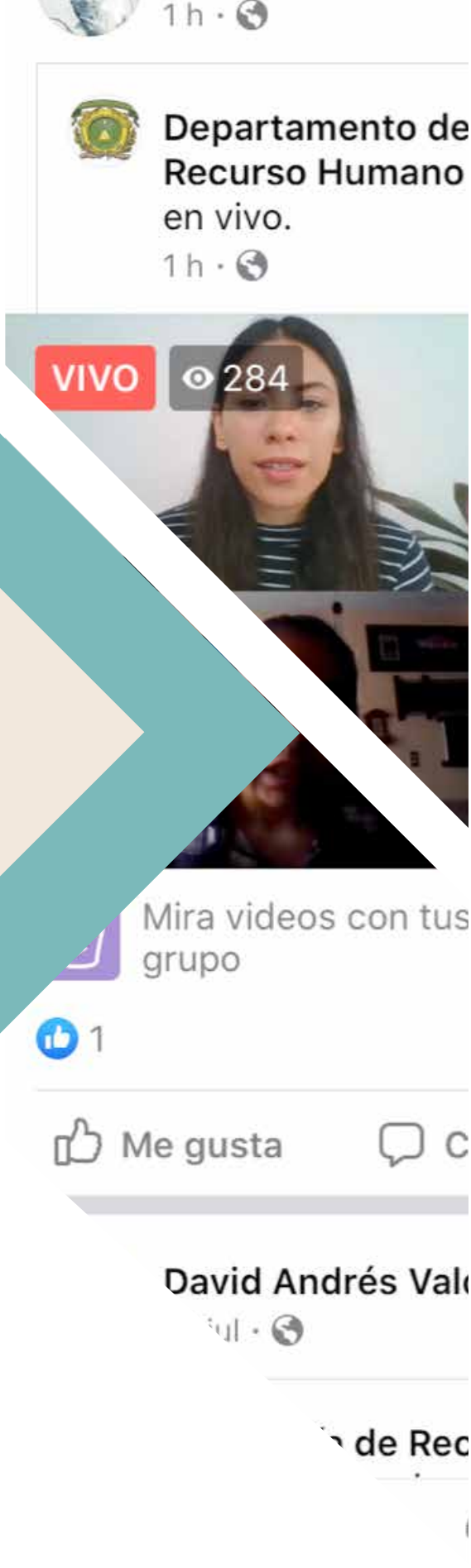
metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

www.incibe.es



ÍNDICE

1. El valor de las redes sociales pág. 03

2. Posibles riesgos de su uso pág. 04

2.1. Error humano pág. 04

2.2. Configuraciones de privacidad débiles pág. 04

2.3. Campañas de fraude: malware y phising pág. 05

3. Medidas de seguridad pág. 06

3.1. Contraseña de acceso pág. 06

3.2. Sentido común pág. 07

3.3. Privacidad pág. 07

3.4. Malware y enlaces pág. 08

4. Referencias pág. 09

1. EL VALOR DE LAS REDES SOCIALES

Actualmente, las redes sociales se han convertido en una herramienta muy importante para la sociedad, y la comunidad universitaria no iba a ser menos. Mediante las redes sociales los estudiantes, docentes, investigadores o personal de administración y servicios pueden realizar contactos, compartir opiniones, estudios, proyectos, eventos, etc. tanto de su vida personal como profesional.

Son muchas las ventajas que pueden aportan las redes sociales, entre otras:

- Compartir conocimiento e información
- Oportunidades laborales
- Información y entretenimiento
- Fomentar la comunicación y colaboración

No obstante, las redes sociales también pueden suponer un riesgo, una mala gestión de las mismas, un comentario inoportuno o los ciberdelincuentes pueden afectar negativamente a la imagen o a la reputación de una persona.

2. POSIBLES RIESGOS DE SU USO

Generar una imagen y una reputación en las redes sociales no es tarea fácil y lo que ha costado esfuerzo y tiempo en crear se puede perder en un instante por un fallo o una mala gestión. Las siguientes circunstancias suponen riesgos en el uso de las redes sociales.

2.1. Error humano

Muchos de los incidentes que afectan a la reputación y a la seguridad en las redes sociales tienen su origen en el error humano. Como por ejemplo el **intercambio de comentarios con un tono elevado.**

Otro error humano que afecta a la seguridad en las redes sociales es **hacer pública información que debería ser privada.**

2.2. Configuraciones de privacidad débiles

Tener una **configuración de privacidad débil** en los perfiles personales o profesionales de redes sociales, es un riesgo para la seguridad de los mismos. Cada red social tiene opciones de privacidad que deben ser revisadas.

Como en cualquier servicio que requiere credenciales de acceso, utilizar una **contraseña débil** puede poner en riesgo tu perfil. Si las credenciales son robadas o se usan contraseñas fáciles de intuir, cualquiera podría publicar en tu nombre o comunicarse con tus seguidores.

Las **aplicaciones** que tienen acceso a los perfiles de redes sociales también pueden suponer un riesgo para la privacidad, ya que podríamos otorgarles acceso (permisos) a determinados datos (como por ejemplo seguidores) que se deberían mantener en privado.

2.3. Campañas de fraude: malware y phising

Los ciberdelincuentes también acechan en las redes sociales mediante diferentes tipos de campañas. Los fraudes que realizan pueden ser llevados a cabo de varias formas, pero el objetivo final siempre será su propio beneficio económico. Para obtener este beneficio, los ciberdelincuentes cuentan con varios métodos:

- **Campañas de malware.** El **envío de software malicioso** por medio de los perfiles en redes sociales también es utilizado por los ciberdelincuentes para **infectar los equipos de las víctimas.** Para engañar a las víctimas utilizan diferentes técnicas como hacerse pasar por una universidad, una empresa, etc. Terminan dirigiendo a la víctima a sitios web maliciosos donde descargarán el malware al hacer clic en un anuncio o simplemente por visitarla. En otros casos, lo envían adjunto en mensajes privados dando como resultado, en ambos casos, la infección del equipo.

- **Campañas de phishing.** Los ciberdelincuentes pueden hacerse pasar por una marca conocida y redirigir a la víctima a una página web fraudulenta donde **robar información personal, bancaria y otro tipo de datos.**

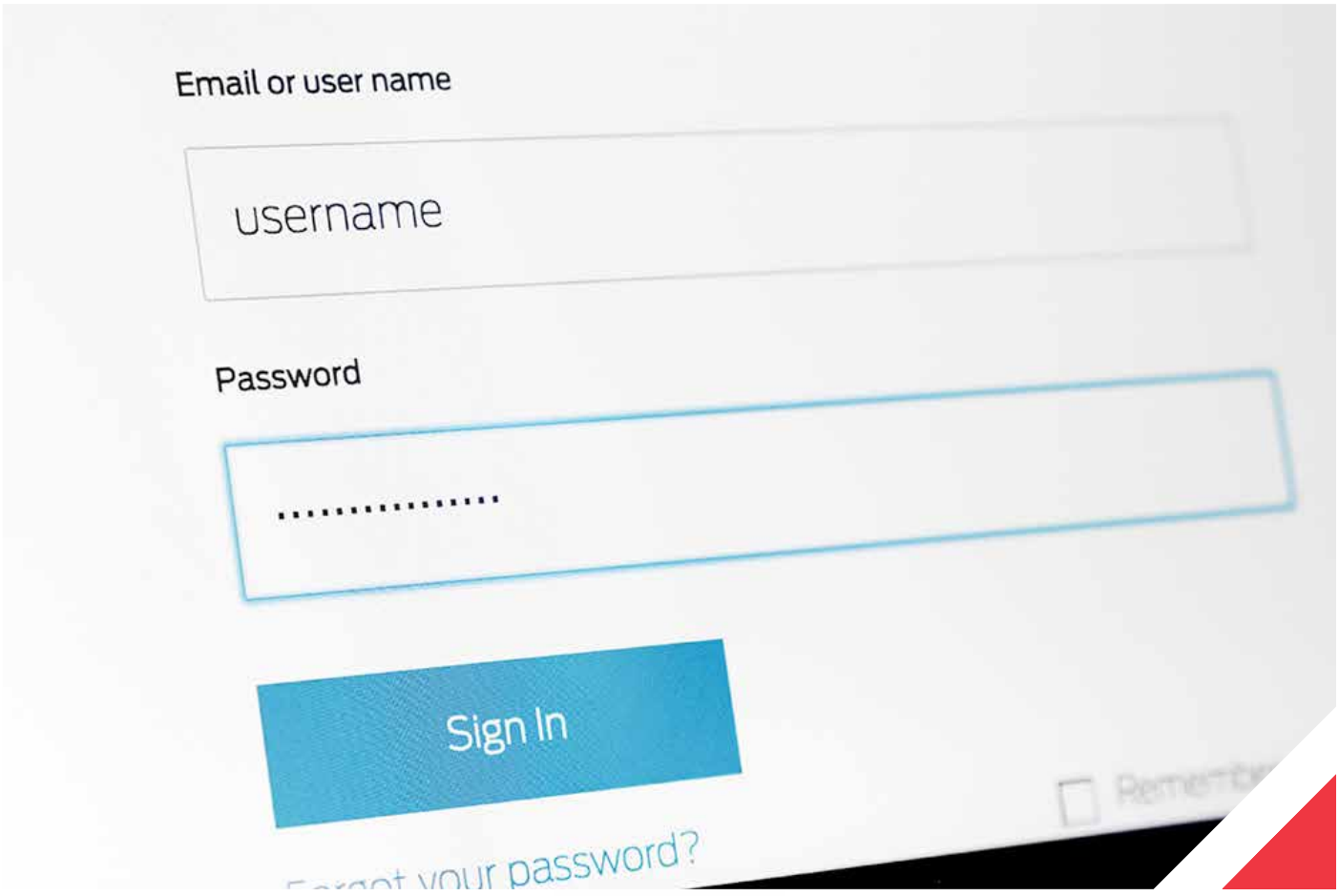
3. MEDIDAS DE SEGURIDAD

Los riesgos anteriores pueden afectar a la reputación de estudiantes, docentes, investigadores o personal de administración y servicios que utilicen las redes sociales. Para evitarlos tendremos que tomar algunas medidas.

3.1. Contraseña de acceso

El primer aspecto a tener en cuenta como en cualquier servicio o aplicación es requerir una **contraseña de acceso robusta.** En este caso, la contraseña es la llave de acceso a la red social. Si alguien no autorizado accede al perfil de nuestra red social podría publicar en nuestro nombre o acceder a nuestros seguidores mediante mensajes directos, deteriorando nuestra imagen.

La mayoría de redes sociales permiten **habilitar el doble factor de autenticación,** que obliga a tener, además de la contraseña, otro factor (huella, código de un solo uso, etc.) para permitir el acceso. Siempre que sea posible se activará. Así, en caso de que la contraseña sea capturada por un ciberdelincuente, no tendrá acceso si no conoce el segundo factor.



3.2. Sentido común

El sentido común es una de las mejores herramientas que se tienen en ciberseguridad, y en el uso de las redes sociales también aplica. Antes de publicar cualquier información tenemos que pensar si puede ser usada en contra o puede afectar negativamente a nuestra imagen. Debemos evitar:

- lanzar comentarios inoportunos, negativos o inapropiados
- enfrascarnos en discusiones sin sentido, insultar, amenazar o acosar;
- propagar noticias falsas;
- dar información confidencial, personal o sujeta a propiedad intelectual, etc.

3.3. Privacidad

Configurar correctamente las opciones de privacidad de tu perfil reducirá, en gran medida, los intentos de fraude por parte de ciberdelincuentes. Las opciones de privacidad deben estar configuradas lo más restrictivamente posible.

3.4. Malware y enlaces

El malware también se ha colado en las redes sociales. Los ciberdelincuentes tienen dos métodos, principalmente, para difundir este tipo de **software malicioso, mediante documentos adjuntos en mensajes dentro de la propia red o por medio de sitios web de terceros.**

Cualquier tipo de documento adjunto enviado por la red social se ha de considerar como una potencial amenaza y se tomarán todas lasmedidas de seguridad necesarias como analizarlo con el antivirus o con herramientas como Virustotal **[Ref. - 1].** También se prestará especial atención a la extensión del archivo. Ante la menor duda no se ejecutará el archivo adjunto. Además, los dispositivos desde los que se utilicen redes sociales, como sucede con cualquier otro dispositivo, siempre deben contar con soluciones antimalware, sistema operativo y otro software actualizado.

De manera similar, sucede con los enlaces, estos pueden redirigir a sitios web fraudulentos de tipo phishing o a sitios web donde descargar archivos infectados. Ante la menor duda con el enlace se evitará acceder al sitio web.

4. REFERENCIAS

1. VIRUSTOTAL - https://www.virustotal.com/gui/home/upload