REDES SOCIALES

Medidas de seguridad para los perfiles de tu universidad

UTTT Universidad Tecnológica de Tula-Tepeji
metared
INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE
incibe_
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
www.incibe.es

ÍNDICE

1. EL VALOR DE LAS REDES SOCIALES

Actualmente, las redes sociales se han convertido en una herramienta muy importante para las universidades permitiendo dar a conocer sus servicios y un trato más cercano con la comunidad universitaria.

Son muchas las ventajas que aportan las redes sociales a una universidad:

- Mediante la analítica del uso de las redes sociales se pueden obtener datos sobre las características de los seguidores como género, edad o ubicación y sus preferencias de uso, que pueden ser útiles a la hora de comunicar la información, servicios y novedades de la universidad.
- También son una buena herramienta para conocer lo que piensa la comunidad universitaria sobre los servicios que ofrece la universidad.
- Permiten aumentar el tráfico web haciendo que la web de la universidad se posicione mejor en los buscadores y aumentando así su visibilidad.
- Sirven para potenciar la marca de la universidad mediante las interacciones de los propios usuarios de la red social.

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

2. POSIBLES RIESGOS DE SU USO

Generar una imagen y reputación de la universidad 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 para la universidad en el uso de las redes sociales. Estos son los principales riesgos asociados a los dispositivos móviles y al teletrabajo:

2.1. Error humano

Muchos de los incidentes que afectan a la reputación y a la seguridad de la universidad en las redes sociales tienen su origen en el error humano. Algunos de los errores más habituales que se producen consisten en **publicar juicios de valor personal en representación de la universidad y el intercambio de comentarios con un tono elevado.**

Otro error humano que afecta a la seguridad de la universidad, y que se comete tanto a través del perfil de la universidad, como del personal de los empleados, es **hacer pública información que debería ser privada**. En otros casos publicar detalles sobre la universidad o del evento al que se va a acudir puede ser usado por un ciberdelincuente para atacar a la universidad.

2.2. Configuraciones de privacidad débiles

Tener una **configuración de privacidad débil** en los perfiles profesionales de redes sociales, es un riesgo para la seguridad la universidad y para la imagen que se quiere proyectar a la comunidad universitaria. 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 el perfil de la universidad. Si las credenciales son robadas o se usan contraseñas fáciles de intuir, cualquiera podría publicar en nombre de la universidad o comunicarse con nuestros seguidores.

Permitir que **cualquier empleado pueda publicar en la página o grupo de la universidad** puede ser un riesgo, ya que la imagen que se quiere dar al público terminará diluyéndose. La universidad debe definir la imagen que quiere dar, qué se publica y qué no, en qué tono o lenguaje, cómo se responde a los seguidores y a las quejas, etc. Solo empleados autorizados y conocedores de ello deben publicar contenidos.

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

2.3. Campañas de fraude: suplantación, 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:

- **Fraude por suplantación.** Los ciberdelincuentes pueden crear **perfiles falsos suplantando a la universidad** para modificar datos en su beneficio. Podría modificar, por ejemplo, los datos de contacto (teléfono, e-mail, etc.).

- **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 la universidad. 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 la universidad y redirigir a la víctima a una página web fraudulenta donde **robar por ejemplo información personal o bancaria.**

3. MEDIDAS DE SEGURIDAD

Los riesgos anteriores pueden afectar a la reputación de la universidad, además de causar infecciones por malware, fugas de información y otros incidentes de seguridad. Para evitarlos tendremos que tomar algunas medidas.

3.1. Contraseña de acceso

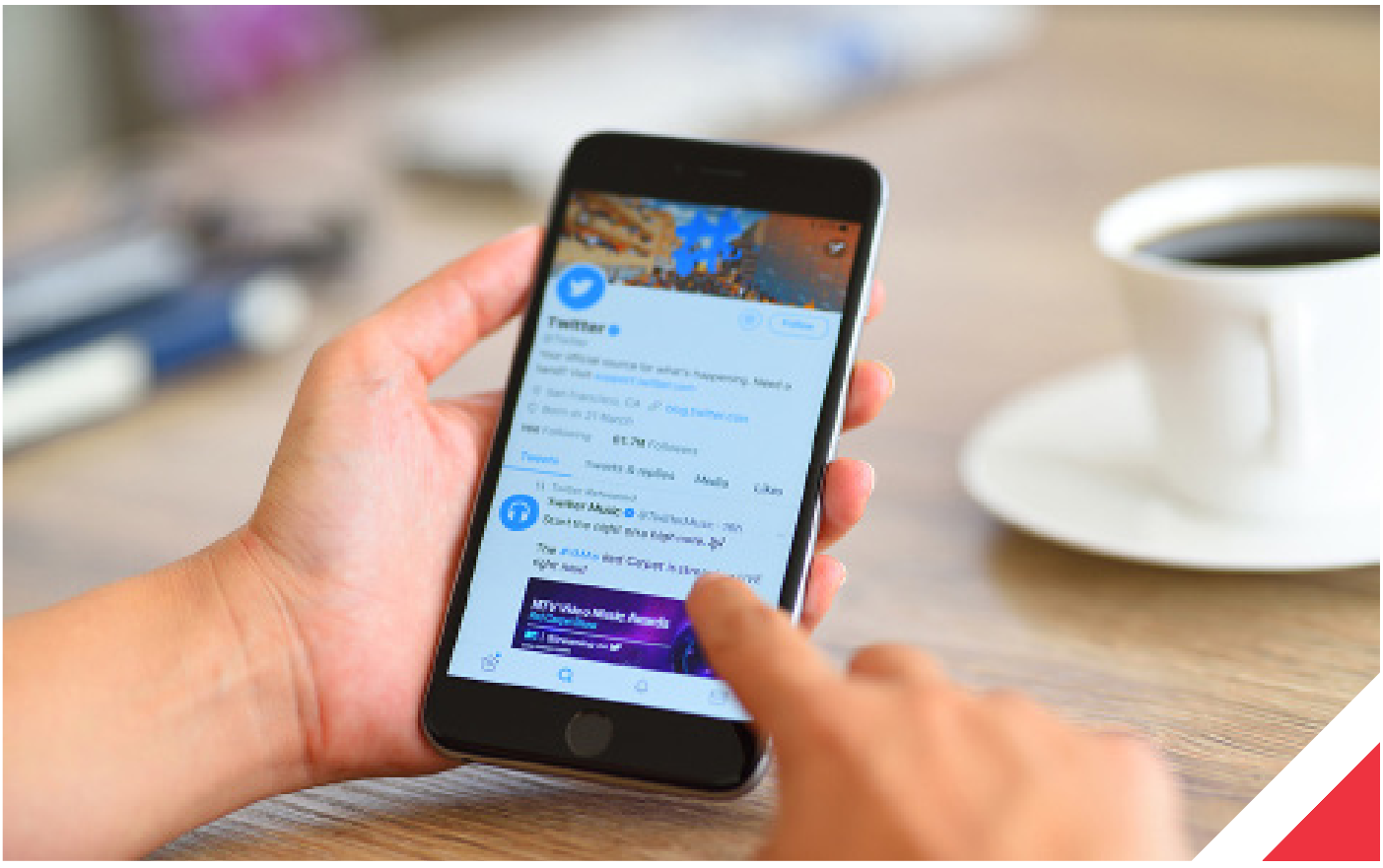
El primer aspecto a tener en cuenta como en cualquier servicio o aplicación que se use en la universidad es requerir una **contraseña de acceso robusta.** En este caso, la contraseña es la llave de acceso a la red social. Si alguien no autorizado accede al perfil de nuestra red social podría publicar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

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 de la universidad o en nombre de ella, tenemos que pensar si puede ser usada en contra o puede afectar negativamente a la imagen de esta. Por el bien de la universidad y porque pueden ser constitutivos de delito, debemos evitar:

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



3.3. Privacidad

Configurar correctamente las opciones de privacidad de los diferentes perfiles reducirá, en gran medida, los intentos de fraude por parte de ciberdelincuentes. **Las opciones de privacidad deben estar configuradas lo más restrictivamente posible,** sin que llegue a afectar al objetivo fijado por la universidad para la red social, como puede ser comunicarse con nuestros seguidores y establecer una relación más cercana.

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.

6. REFERENCIAS

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