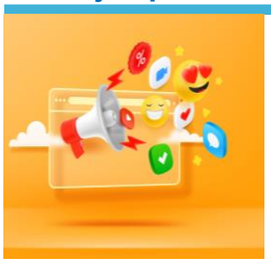
Advertencia de Seguridad

Consejos para Community Managers: Aseguramiento de redes y presencia digital.

COLCERT AD-2310-024

TLP:CLEAR



La presencia en redes sociales es indispensable para las organizaciones y entidades, ya que facilita la comunicación y el alcance a un público amplio. Sin embargo, esta presencia también conlleva un alto nivel de criticidad debido a las amenazas cibernéticas que pueden afectar negativamente la imagen y la reputación online.

Por lo tanto, es crucial implementar hábitos cotidianos de ciberseguridad para proteger las cuentas y la información. Estos hábitos incluyen el uso de contraseñas robustas, la activación de la autenticación en dos pasos, la educación continua sobre phishing y otras tácticas de ingeniería social y la revisión regular de las configuraciones de privacidad.

Principales riesgos de ciberseguridad para Community Managers.

- **Secuestro de cuentas (Account Hacking).**

  Los perfiles en redes sociales son objetivos frecuentes de los ciberdelicuentes, que buscan acceso no autorizado para suplantar la identidad de la marca, empresa, entidad o persona y así publicar contenido malicioso o robar información confidencial.

- **Suplantación de identidad.**

  Los community managers pueden ser víctimas de correos electrónicos o mensajes engañosos diseñados para robar credenciales de inicio de sesión o datos sensibles. Esto puede llevar a la pérdida de control sobre las cuentas.

- **Vulnerabilidades en aplicaciones de terceros.**

  Herramientas de gestión de redes sociales, como las plataformas de programación o análisis, pueden tener fallos de seguridad. Si estas plataformas son comprometidas, los atacantes podrían acceder a las cuentas vinculadas, generando riesgos que pueden afectar tanto la reputación como la seguridad de la información manejada por el community manager.

Estas son algunas recomendaciones esenciales para fortalecer la seguridad digital.

- **Autenticación de dos factores (2FA).**

  Implementar la autenticación de dos factores (2FA) en todas tus plataformas, como X, Instagram, Facebook y TikTok, es una medida esencial para mejorar la seguridad de las cuentas. Esta función añade una capa adicional de protección al requerir no solo tu contraseña, sino también un código temporal que se genera en tiempo real. De esta manera, incluso si alguien obtiene la contraseña, no podrá acceder a la cuenta sin el código temporal, lo que reduce significativamente el riesgo de accesos no autorizados.

- **Contraseñas Seguras y únicas.**

  Es importante utilizar contraseñas seguras y únicas. Asegúrate de que las contraseñas sean robustas, compuestas por una combinación de letras, números y caracteres especiales, evitando palabras y combinaciones comunes o de fácil acceso.

  No usar la misma contraseña en diferentes plataformas y cambia las contraseñas regularmente para mantener la seguridad de las cuentas.

COLCERT

Advertencia de Seguridad

Consejos para Community Managers: Aseguramiento de redes y presencia digital.

COLCERT AD-2310-024

❑ Permisos de acceso controlados.

Si trabajas con un equipo, es necesario asegurarse de que solo las personas necesarias tengan acceso a las cuentas. Usar herramientas de gestión de redes sociales que permitan asignar roles con distintos niveles de acceso sin compartir directamente las credenciales. Esto no solo mejora la seguridad, sino que también facilita la administración y el control de las cuentas.

❑ Vigilancia del contenido y mensajes privados.

Evitar hacer clic en enlaces sospechosos enviados a través de mensajes directos, ya que este es un método común para ataques de phishing. Verificar las URL antes de hacer clic, ya que los atacantes pueden usar sitios que imitan plataformas populares para robar datos. Además, mantener una vigilancia constante sobre el contenido y los mensajes privados.

Revisar regularmente los mensajes y publicaciones para detectar cualquier actividad inusual o sospechosa. Configurar alertas para notificaciones de inicio de sesión y cambios en la cuenta. Usar herramientas de monitoreo que te permitan rastrear menciones y actividades relacionadas con tus cuentas para detectar posibles amenazas a tiempo

❑ Protección de Dispositivos.

Mantener actualizados los dispositivos y las aplicaciones que se usan para gestionar redes sociales, ya que las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades. Usar software antivirus y firewalls para protegerte contra malware. Evitar usar dispositivos personales para la gestión de los contenidos, ya que esto puede aumentar el riesgo de exposición a amenazas de seguridad.

FUENTES:

https://blog.hootsuite.com/es/riesgos-de-seguridad-en-redes-sociales/

https://www.incibe.es/sites/default/files/contenidos/guias/doc/GU%C3%8DA_CIBERSEGURIDAD_EN_LA_IDENTIDAD_DIGITAL.pdf

COLCERT