INSTITUTO DE INVESTIGACIONES SOCIALES

COMISIÓN LOCAL DE SEGURIDAD INSTITUTO DE INVESTIGACIONES SOCIALES

PROTOCOLO EN CASO DE AMENAZAS EN REDES SOCIALES.

Concientizar y otorgar información que permita evitar amenazas a través de las redes sociales, así como, sus consecuencias que afecten a la comunidad de este instituto.

INSTITUTO DE INVESTIGACIONES SOCIALES

ID del Documento: KLUKR8Wpz2GoIyBP1OhlpS6qOEGmfKXAAuIN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —25 de 42—

Contenido

Definición. 2

Objetivo. 4

Alcance. 4

Participantes. 4

Capacitación. 4

Medidas preventivas de seguridad. 5

Actuación en caso de amenaza por red social. 5

Teléfonos de emergencia. 6

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —26 de 42—

Definición.

Se define como amenaza el "*anuncio de un mal dirigido a otro, que puede realizarse de forma oral, escrita o con actos y con entidad suficiente para infundir miedo y temor*" (Real Academia Española, 2020), las cuales pueden estar motivadas por allanamiento, sabotaje, robo, fraude, espionaje, la exigencia de dinero o algún otro delito; y puede ser grave cuando es efectuada de forma seria, real y persistente, atentando contra la salud o vida de la víctima o sus familiares.

Existen diferentes tipos de amenazas, pero las más comunes son:

Amenazas con revelar información de otro. Cuando alguien exige una cantidad o recompensa bajo la amenaza de difundir información o hechos referentes a su vida privada que no sean públicamente conocidos y puedan afectar de cualquier manera (física, mental o socialmente) a la persona, conocidos o familiares.

Amenazas contra la pareja. Cuando de modo leve o severo se atente (física o emocionalmente) con quien tenga o haya tenido una relación sentimental con el fin de perjudicar su persona o su prestigio.

Amenazas con armas o instrumentos peligrosos. Es el uso de armas de cualquier índole u objetos peligrosos con el fin de obtener algún beneficio o bien material de la víctima.

Hoy en día las amenazas no únicamente son recibidas de manera presencial, han comenzado a transformarse con la popularización de las redes sociales como Facebook, Twitter, Instagram, Pinterest, Youtube, SnapChat, TikTok y, especialmente, el servicio de WhatsApp, las cuales han permitido que estas intimidaciones o chantajes sean realizadas a través de medios escritos, digitales o auditivos en contra de alguna o varias personas, por lo cual, es necesario conocer de forma básica como funcionan los aspectos de seguridad de éstas para poder orientar a los usuarios en un manejo responsable y seguro.

Si bien la finalidad de las redes sociales es el entretenimiento o la absorción de información, es a través de la interacción entre usuarios, donde se esconden varios riesgos al interactuar con personas desconocidas o incluso conocidas, por ejemplo, el uso del sistema de geolocalización que requieren algunas aplicaciones para mostrar la distancia aproximada en el que se encuentra un usuario de otro o de alguna ubicación, o el uso de redes abiertas de internet en lugares públicos que también propicia un posible robo de información personal. Sin embargo, existen riesgos que se presentan cada vez más frecuentes, tales como:

***Sexting*.** Publicación de fotografías con fines "sexuales" o de "coqueteo".

Grooming. Acciones emprendidas por un adulto para ganarse la confianza de un menor y tratar de conseguir una cita para abusar sexualmente de él, extorsionarlo o incitar al sexting, entre otras acciones.

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —27 de 42—

Ciberbullying. Ciberacoso psicológico, generalmente entre los menores de edad, usando los canales sociales y de mensajería.

Hacking. Suplantación de la identidad al acceder a las cuentas o perfiles de los usuarios.

Phishing. Obtención de datos personales a través de web ficticias con el fin de realizar hacking sobre alguna persona.

En el caso particular del Instituto de Investigaciones Sociales, es de suma importancia abordar dos puntos que en el contexto en redes sociales pudieran existir con mayor frecuencia:

Difamación por comentarios*: refiere a la* posibilidad de recibir diversos comentarios negativos a través de posts, historias o videos debido al carácter público de las cuentas del Instituto *y que tengan la intención de dañar o difamar a una o varias personas.*

Riesgo de phising: *este tipo de amenaza se presenta a través de mensajes de texto, correos o mensajes contienen links de un remitente desconocido, que tienen intenciones maliciosas, de robo de información o suplantación de identidad.*

Por lo anterior que en páginas siguientes se presenta el **Protocolo Por Amenazas En Redes Sociales Del Instituto De Investigaciones Sociales** con el fin de prevenir, actuar y atender de manera rápida y eficiente cualquier caso que se presente.

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —28 de 42—

Objetivo.

Plantear los lineamientos para prevenir y/o subsanar las acciones por amenaza a través de redes sociales para la comunidad del Instituto de Investigaciones Sociales (IIS).

Alcance.

El propósito de este documento es concientizar y otorgar información que permita evitar amenazas a través de las redes sociales, así como, sus consecuencias que afecten a la comunidad de este instituto.

Participantes.

- Comunidad universitaria: personal académico y administrativo.
- Titular del Instituto de Investigaciones Sociales.
- Secretario Administrativo del IIS.
- Oficina Jurídica de la Coordinación de Humanidades.
- Brigadistas.
- Personal de vigilancia.
- Dirección General de Análisis, Protección y Seguridad Universitaria (DGAPSU).
- Personal adscrito a la Fiscalía y/o secretaria de seguridad pública o ciudadana, federal o local.

Capacitación.

Se recomienda capacitar y actualizar permanentemente al personal académico, administrativo y de toma de decisiones del Instituto que participen en la actuación de este protocolo, en los siguientes temas:

- Curso de redes sociales.
- Acciones que seguir ante amenazas a través de redes sociales.
- Atención a crisis de las víctimas.

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —29 de 42—

Medidas preventivas de seguridad.

- El titular del Instituto en coordinación con la Comisión Local de Seguridad promoverá las siguientes medidas de prevención que, están basadas en las recomendaciones generales de la Policía Ciberdelincuencia Preventiva, dependiente de la Secretaría de Seguridad Ciudadana de la Ciudad de México, así como de la policía del ámbito federal.
- En redes sociales, evitar aceptar solicitudes de desconocidos.
- Evitar publicar información de índole estrictamente personal.
- De ser posible, evitar publicar información y fotografías de familiares.
- Pensar dos veces antes de escribir una publicación.
- Comprobar la configuración de privacidad en cada una de las redes sociales y apps.
- Evitar el uso indebido del correo institucional.
- Notificar al área de cómputo, difusión o dirección cuando reciba un link de un remitente desconocido.
- No compartir información personal o confidencial con personas desconocidas a través de redes sociales o correo.
- Socialice estas precauciones entre la comunidad universitaria, trabajadores y funcionarios del Instituto.

Actuación en caso de amenaza por red social.

- Mantener la calma y no tomar medidas impulsivas.
- Hacer del conocimiento de los hechos a personas de confianza, quienes además de servir de apoyo podrían fungir como posibles testigos.
- Dar aviso de manera rápida y oportuna a las autoridades del Instituto, quienes pueden ayudar como mediadores de la institución marcando al número de emergencias o a través de la app SOS UNAM.
- Si la amenaza es en contra de algún amigo o familiar y, ésta parece inminente, ponerse en contacto con ellos y explicarles la situación para permanecer seguros. Evitar entrar en pánico para no contagiar a los familiares.
- En caso de amenaza por red social es importante guardar las evidencias, sobre todo si viene de un usuario claramente identificable.
- Para guardar las evidencias de amenaza, especialmente si son reiteradas, basta con hacer una captura de pantalla en el dispositivo o computadora.
- Si se opta por hacer la captura de pantalla, es imperativo que se realice inmediatamente después de leer la amenaza, ya que, de acuerdo con las instancias policiales, los autores suelen borrarlas casi de inmediato, calculando el tiempo necesario para que la víctima lea el mensaje.
- En el caso de mensajes de audio, se recomienda respaldarlos y/o grabarlos. La mayoría de los teléfonos actuales cuentan con alguna aplicación para grabar

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —30 de 42—

audio. De lo contrario, en línea existen diversas apps que tiene este propósito. Se recomienda tener instalada alguna de éstas.

- Una manera apropiada de guardar las conversaciones en la plataforma WhatsApp, es a través de las copias de seguridad. Allí permanecen los textos, imágenes y audios que un posible acosador realice.
- El afectado por la amenaza también puede poner la situación en conocimiento de la red social donde ha sido emitida. Este procedimiento es totalmente anónimo y muy sencillo, basta con pinchar sobre el comentario y denunciarlo como abuso o spam.
- En caso necesario, la Oficina Jurídica de la Coordinación de Humanidades, solicitará el apoyo de la Oficina de la Abogacía General, para que interponga una denuncia ante la Fiscalía.
- Es importante señalar que para que, una denuncia sea procedente se debe contar con pruebas sólidas, por lo que se deben conservar grabaciones de audio, videos, fotografías o capturas de pantalla que reflejen la amenaza.
- Se debe evitar a toda costa el uso de violencia como medida de prevención ante una amenaza, pues se puede cambiar de víctimas a victimarios en instantes.

Teléfonos de emergencia.

911

Denuncia anónima

089

Apoyo disponible las 24 horas del día

Ciudad Universitaria	
Secretaría de Prevención, Atención y Seguridad Universitaria	55 5622 1284 /1286
Sistema de Orientación en Salud	55 56220127
CAE (Central de Atención de Emergencias)	55-56160523, extensiones 0914 y 02989. Desde cualquier extensión UNAM 55
Servicios Médicos Urgencias	Extensiones 20140 y 20202
Sistema de Orientación en Salud	Directo 55-56220127
Protección Civil	55-56226556

ID del Documento: KLUKR8Wpz2ColyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —31 de 42—

Línea de reacción PUMA	55-56226464
Denuncia Universitaria	01800-2264725

Ciudad de México	
Locatel	55 56581111
Protección Civil	55 56832222
Unidad de contacto del Secretario de Seguridad Ciudadana	55 52089898

ID del Documento: KLUKR8Wpz2SolyBP10hfpS6qOEGmfKXAAuN4wcNSvMI=
Fecha de procesamiento: 2024-09-23T13:13:10
Páginas: —32 de 42—