ACTIVIDAD No. 1 DELITOS Y PELIGROS INFORMÁTICOS



¿QUÉ SON LOS DELITOS INFORMÁTICOS?

Con el término delito informático aglutinamos los hechos que, basándose en técnicas o mecanismos informáticos, pudieren ser tipificados como delito en el Código Penal, tales como: delito de estafa, delito contra la propiedad intelectual e industrial, etc. Debido a los avances tecnológicos y a los nuevos mecanismos para delinquir se ha hecho necesario introducir y modificar determinados artículos que permitan aglutinar éstos.

¿CUÁLES DELITOS INFORMÁTICOS SE PRESENTAN CON MAYOR FRECUENCIA?

1. **Información falsa**: El robo de identidad cibernético o también conocido como “catfish” (mentira en la red).
2. **El Phishing:** Conocido también como suplantación de identidad, se utiliza de forma fraudulenta fundamentalmente para poder extraer de manera ilegal información privada o confidencial.
3. **El sexting y el acoso a menores de edad:** Se trata del envío de imágenes o vídeos con contenido sexual, este delito es más común mediante los teléfonos inteligentes. El sexting en adultos, se trata de la difusión sin autorización de imágenes o vídeos en temas sexuales, mediante una red social o informativa de un individuo.
4. **El ciberbullying**: es un término que se le da al acto de acoso, humillación, burla y amenaza que se le da a un niño o adolescente mediante una red social. Por otra parte, existe el
5. **Virus y ataques informáticos:** Los troyanos son un tipo de virus que crecen año tras año; se trata de un virus que toma el control de tu computadora desde un lugar remoto. Por lo general, actúan invitándote a bajar un archivo que te permite acceder a nuevas funcionalidades en Facebook, por ejemplo.



6. **Vulneración a sistemas y páginas web:** En este punto es importante hablar de los famosos cracker quienes son los protagonistas. ¿Qué es un cracker? Un cracker es una persona con altos conocimientos en tema de informática, quien utiliza sus conocimientos para vulnerar y dañar deliberadamente sistemas de seguridad. Los crackers buscan crear caos informático, modificar sistemas, espionaje informático, y estafar.
7. **Publicidad engañosa:** El libre comercio de productos y servicios en Internet ha generado que se

publiquen promociones increíbles, por ofrecer oportunidades únicas de compra a los usuarios, sin embargo, al momento de concretar la compra y hacer el pago no envían el producto o éste no cumple con las características ofrecidas.

8. **Stalking:** Se refiere al hecho de acoso, persecución, contacto intrusivo o constante que una persona hace a otra mediante mensajes a través de las redes sociales.
9. **Ofensas y calumnias**: Una calumnia en las redes afecta la dignidad y altera la estima que se tiene de la víctima. Aunque no parezca un delito grave cuando se sobrepasan los límites y se violan los derechos a la intimidad, de manos de terceros, si lo es. Las personas que cometen estos actos de hostigamiento mediante las redes sociales, comúnmente alegan que están haciendo uso de su derecho de libre expresión. Pero hay una línea bastante difusa en donde se puede sobrepasar los límites y moverse de la libre expresión, al abuso y ofensa hacia otra persona.
10. **Incitación al odio:** En este caso se refiere a todas aquellas personas que utilizan las redes sociales para publicar y distribuir algún tipo de escrito, imagen o vídeo que fomente la humillación, xenofobia o discriminación hacia algo o alguien. Algunos ejemplos, podrían ser escritos de discriminación racial, orientación sexual, religión entre otros casos.
11. 11.**El vídeo virus**: los vídeos se han convertido en atractivos anzuelos para los ataques cibernéticos a desprevenidos.

Prometiendo mostrar vídeos que para nosotros pueden resultar de interés, pero no son otra cosa que un pasaje de ida a la introducción de un virus a la computadora o malware y obtener así datos personales o financieros sin tu autorización.

¿QUÉ HACER SI ERES VICTIMA DE UN DELITO INFORMÁTICO?

- Denunciar en el CAI virtual o Centro Cibernético Policial, el cual tiene un servicio para reportar delitos informáticos y el hurto de equipos móviles.
- Si se publican imágenes, datos sensibles, datos personales sin autorización de la víctima, se debe hacer una denuncia ante la Fiscalía por el delito de violación de datos personales.
- Si el acoso está relacionado con un acceso abusivo a una cuenta de correo electrónico, un celular o el perfil en una red social, se puede denunciar el hecho ante la Fiscalía, pues podría tratarse del delito de acceso abusivo a sistema informático.
- Si el acoso involucra otras conductas como maltratos psicológicos u ofensas, también se puede denunciar por los delitos de injuria y calumnia. Adicionalmente, se puede instaurar una queja ante la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio, la cual tiene como función proteger los datos personales de los colombianos.
- Si el ciberacoso involucra a un menor de edad, se debe acudir a las autoridades y recordar que existe una protección especial para los menores de edad, como el Código de Infancia y Adolescencia y las leyes contra la pornografía infantil. Existen sitios como teprotejo, que se enfocan en la prevención y protección de menores de edad.



OTRAS RECOMENDACIONES

Para prevenir un ciberacoso, siempre se debe partir del supuesto que se debe entregar la mínima información posible que pueda llevar a un acoso digital. Se recomienda no compartir fotografías íntimas, o datos sensibles o personales que puedan llevar a comprometer a una persona. La mejor forma de evitar un ciberacoso es la desconfianza. No se trata de volverse paranoico, ni mucho menos de alejarse de los medios electrónicos. La mejor prevención es estar alerta: revisar todo lo que hacemos en internet, cómo compartimos la información y con quién lo hacemos. No entregues información personal sensible a sitios que desconozcas, crea cuentas de correo electrónico diferentes para registrarte en redes sociales e, incluso, considera la posibilidad de usar nombres

diferentes al tuyo. Busca tu nombre en Google o en buscadores con regularidad, en caso de que haya una filtración indeseada. En suma: cuida tus datos personales. Y siempre recuerda que compartir información con contenido sexual hace que otros la puedan aprovechar en tu contra. El amor no dura para siempre.



AHORA TE TOCA A TI ACTIVIDAD No 1

Responde las preguntas según la lectura anterior

En Word y el cuaderno:

1. Realiza un mapa conceptual del tema.
2. Realiza una sopa de letras con los delitos del texto.
3. Escribe a qué tipo de Delito corresponden los siguientes enunciados:

a) Mariana recibió la solicitud de amistad en su red social de una persona que ella cree es del colegio por su foto de perfil, ella lo acepta como amigo, pero al entablar una conversación se da cuenta que no es quien ella piensa. Alguien la suplantó.

b) Oscar recibió en su red social una promoción fabulosa para comprar unos celulares de última generación muy baratos; él los compró por internet, pero nunca llegaron.

c) A Fabio le llegó a su perfil el enlace para descargar un vídeo de situaciones muy graciosas de algunos deportistas, motivado por la curiosidad lo descargó y ahora su computador no funciona muy bien.

d) Juan y María eran novios, y al terminar su relación Juan difundió sin autorización de María algunas imágenes con contenido sexuales.

e) Desde hace un tiempo Juliana ha estado recibiendo en su red social mensajes de acoso, ya se siente hostigada y perseguida.

f) En un acto cultural realizado en el colegio, Yulieth participó en un baile, fue grabada por algunos compañeros que compartieron el video en las redes sociales, desde entonces Yulieth ha sido blanco de humillaciones y burlas por parte de conocidos y desconocidos que vieron su video.

4. Realiza un folleto o plegable bien creativo y presentable teniendo en cuenta los delitos informáticos, usando texto, imágenes, líneas de atención y también consultando la legislación en Colombia sobre los delitos informáticos, sus consecuencias legales y/ o penales

Enviar el documento al correo JULIO.ZUNIGA@FEYALEGRIALACIMA.EDU.CO