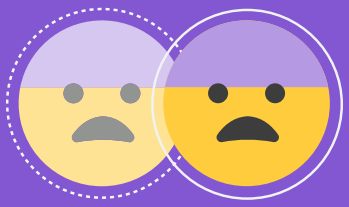

Tipología de Ataques Digitales

PROTEGE.LA

SOCIALTIC

GOBIERNO DE LA CIUDAD DE MÉXICO

MPI CDMX

Elaborado por:

Haydeé Quijano

Juan Manuel Casanueva

Paul Aguilar

Publicado en julio 2020 en protege.la

La tipología de ataques digitales está publicada en línea en: https://protege.la/ataques/

PROTEGE.LA

SOCIALTIC

GOBIERNO DE LA CIUDAD DE MÉXICO

MPI CDMX

Contenido:

Contenido:

Objetivo:

En un espectro de violencia donde las agresiones toman distintas formas, son múltiples y se relacionan, esta tipología busca describir cómo funcionan los ataques digitales, algunos de los riesgos que conllevan y medidas digitales de prevención.

¿Qué es un ataque digital?

Cualquier acción y comportamiento con fines maliciosos mediante el uso de tecnologías de la información y la comunicación (TIC), como teléfonos, sitios web, plataformas de redes sociales y/o correos electrónicos.

Los ataques o agresiones digitales tienen como fin generar, incitar o agravar un daño. Y suelen enfocarse a intimidar, insultar/avergonzar, calumniar/desprestigiar, silenciar/censurar, chantajear/extorsionar, conseguir o robar información.

Categorías

Ataques digitales mediante vulneraciones técnicas: Implican abusar del diseño de la tecnología para modificar o romper aspectos técnicos con fines maliciosos.

Ataques digitales mediante conductas humanas: Implican abusar o aprovecharse del componente humano y las relaciones sociales con tal de generar un daño.

Generalmente las dos categorías de ataques se relacionan entre sí.

Aspectos a considerar

a) Enfoque descriptivo

- Los ataques aquí descritos abordan de manera general el cómo se manifiestan, buscando ser útil como punto de inicio para un diagnóstico más profundo.
- Cada ataque está descrito por individual, sin embargo se debe tener en cuenta ataques que se combinan o cruzan y cómo derivan en otras manifestaciones y riesgos.
- Contemplamos algunos posibles riesgos, ya que el impacto es de manera diferenciada, según quien las ejerce, quien las vive y en qué contexto social, cultural, económico, político están teniendo lugar. Por lo que al realizar un análisis de riesgo, es importante identificar otras vulneraciones según el contexto.
- Al utilizar esta tipología para documentar ataques digitales es clave tener en cuenta cómo se atacan grupos y comunidades específicas, por ejemplo mujeres y comunidades de diversidad sexual. Por lo que esta tipología tendrá que abordarse desde una perspectiva de género e interseccionalidad.
- Las medidas de prevención son algunas propuestas. Para una prevención y atención integral, se deben incluir aspectos físicos, digitales y emocionales de acuerdo a cada caso.

b) Capacidad del agresor

Esta tipología está desarrollada y ordenada considerando las capacidades del agresor, su objetivo y cómo algunos ataques pueden habilitar a otros de manera escalonada. Así como la coordinación y estrategia del agresor/es.

c) Agravantes

Cualquier ataque puede agravar el impacto sobre la víctima u objetivo a través de:

- La combinación y/o cruce ataques
- El volumen, persistencia o mayor cantidad de relación entre ataques
- El contexto de quien es objetivo y vive los ataques así como de quien los ejerce

Ataques digitales mediante

Vulneraciones Técnicas

Implican el uso de una o varias técnicas para abusar del diseño de la tecnología para modificar o romper aspectos técnicos con fines maliciosos.

Daño o pérdida de dispositivos

Descripción:
En los equipos, como computadora, celular, discos o USB, guardamos grandes cantidades de información. Estos equipos son una puerta a la actividad personal, laboral y de redes de contactos. En caso de daño o robo de equipos, se puede perder esta información y/o alguien más podrá tener acceso a ella y utilizarla con fines maliciosos.

Ej. robo en la calle, transporte público, vehículos privados, habitación o allanamientos de oficinas.

Ej. daño por violencia física en manifestaciones, espacios privados o públicos.

Posibles riesgos:

- Pérdida de información por daño (parcial o total) o robo de la misma.
- Filtración o exposición de información.
- Acceso a información privada o sensible.
- Si la información es sensible, se compromete la integridad de una persona o grupo.
- Debido al acceso a la información, se pueden generar campañas de censura y desprestigio.

Medidas de prevención:

- Respaldar periódicamente la información en medios de almacenamiento externos y en lugares a salvo de daños y robo.
- Elegir el lugar y medio de almacenamiento adecuado en función de la información que se desea proteger o resguardar.
- Bloquear el acceso a dispositivos configurando usuarios y contraseñas seguras.
- Cifrar la información privada y sensible (el cifrado asegura la información con candados y códigos especiales para protegerla).

Accesos no autorizados dispositivos, cuentas y servicios en línea

Descripción:

Un acceso no autorizado a cuentas y servicios en línea, puede de manera directa o indirecta brindar información específica de una persona y comprometer su seguridad e integridad. Un acceso no autorizado se puede dar por filtraciones o robo de usuarios y contraseñas, o por ataques de fuerza bruta, que son mecanismos automatizados con programas de computadora para probar combinaciones de contraseñas mediante diccionarios.

Ej. acceso a cuentas en línea de redes sociales, servicios de correo o sitios web.

Posibles riesgos:

- Acceso a información privada o sensible.
- Filtración o exposición de información.
- Se pueden generar campañas de censura y desprestigio.
- Suplantación de identidad.
- Espionaje y monitoreo.

Medidas de prevención:

- Utilizar contraseñas seguras
  - Que combinan caracteres alfanuméricos y símbolos, con una longitud mayor de 8 caracteres. Ej. C0ntr4s3ñ4sS3gur4s!
  - Únicas
  - Privadas
  - Con caducidad (que cambien por lo menos una vez al año)
- Utilizar la verificación de dos pasos
- Revisar periódicamente en las cuentas (cada 6 meses):
  - Conexiones e inicios de sesión
  - Configuraciones de seguridad
  - Configuraciones de privacidad
- Evitar caer en phishing.
- Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

(Phishing) Suplantación y falsificación de información, servicios o sistemas

Descripción:

El phishing es una técnica que se basa en suplantar o falsificar información para incitar a la persona a realizar una acción, como dar clic a un enlace, abrir un archivo infectado o conectarse a una red o sistema falso. Generalmente con el objetivo de robar información, infectar un equipo o sistema de información.

Ej. correos electrónicos o sms sospechosos solicitando dar clic a enlaces.

Ej. correos electrónicos o sms sospechosos solicitando enviar o responder información privada, sensible o financiera.

Ej. correos electrónicos sospechosos solicitando abrir archivos adjuntos.

Posibles riesgos:

- Robo de información
- Robo de datos para iniciar sesión en cuentas
- Accesos no autorizados a cuentas
- Suplantación de identidad
- Infecciones e intervenciones de sistemas y equipos

Medidas de prevención:

- Verificar e identificar:
  - Origen de la información (emisor)
  - Veracidad del contenido
  - Veracidad de los enlaces o adjuntos
- En caso de reconocer información sospechosa o poco confiable, evitar dar responder, dar clic en enlaces o abrir archivos adjuntos.
- Evitar compartir información privada o sensible en espacios digitales.

Denegación de servicios

Descripción:
Técnica que busca saturar un servicio o sistema para que colapse y no pueda atender peticiones. Se suele llevar a cabo con ataques de fuerza bruta y son principalmente dirigidos a un objetivo en específico, el servicio. Cualquier servicio en línea accesible de manera pública, puede ser atacado, ya sea un sitio web o un servicio de mensajería.

Ej. Un sitio web recibe un gran volumen de visitas automatizadas y queda fuera de línea.

Ej. Una red de internet como un WiFi en un espacio público recibe un gran volumen de visitas automatizadas y queda fuera de servicio.

Ej. Una red de telefonía móvil recibe un gran volumen de solicitudes o llamadas y ya no puede atender el servicio.

Posibles riesgos:

- Bloqueo parcial o total del servicio
- Pérdida de información en un proceso de comunicación ya que el canal de comunicación está bloqueado
- Suplantación o alteración del servicio
- Se pueden generar campañas de censura y desprestigio

Medidas de prevención:

- Utilizar sistemas que cuenten con infraestructuras robustas y escalables con tal de soportar ataques de gran volumen
- Modificar las configuraciones pre-establecidas de los servicios para que no sean fácilmente detectables
- Monitorear la actividad del servicio o sistema para detectar comportamientos anormales
- Utilizar sistemas de apoyo como un CDN que detectan y bloquean visitas automatizadas (Content Delivery Network) Ej. Deflect y CloudFlare

Intervención para alterar o modificar sistemas o dispositivos

Descripción:

Intervenir un sistema de información (como programas y aplicaciones) y/o equipo de cómputo requiere modificar o alterar su funcionamiento y contenido de manera no autorizada, a través de virus o componentes físicos.

Ej. Infección por virus descargados mediante phishing.

Ej. infección de virus por dispositivos físicos como USB conectados al equipo o dispositivo.

Ej. Modificación física del equipo cambiando sus partes por otras.

Posibles riesgos:

- Instalación o intervención mediante:
  - Virus
  - Inyecciones de código malicioso
  - Accesos de control remoto
  - Accesos no autorizados con permisos de administración
- Daño, modificación o alteración de:
  - Datos e información
  - Programas, aplicaciones y sistemas operativos
- Filtración o exposición de información.
- Acceso a información privada o sensible.
- Si la información es sensible, se compromete la integridad de una persona o grupo.
- Bloqueo parcial o total del sistema o equipo.
- Pérdida de información.
- Suplantación o alteración de la información o los sistemas.
- Espionaje y monitoreo.
- Secuestro de información, sistema o equipo.

Medidas de prevención:

- Respaldar periódicamente la información e infraestructura de los sistemas a medios de almacenamiento seguros.
- Bloquear el acceso a dispositivos configurando usuarios y contraseñas seguras.
- Cifrar la información privada y sensible.
- Instalar actualizaciones de seguridad.
- Instalar y utilizar antivirus y firewalls.
- Evitar caer en phishing.

Intervención para alterar o modificar infraestructuras de comunicación.

Descripción:

Intervenir una infraestructura de comunicación como redes de telefonía fija, móvil e internet, requiere modificar o alterar físicamente su funcionamiento con el fin de interceptar y/o manipular el contenido que viaja en ella.

Ej. instalación de antenas no oficiales (IMSI Catchers , Stingray)

Ej. alteración de las antenas mediante programas u otras antenas repetidoras, para extraer información a fuentes externas.

Posibles riesgos:

- Bloqueo parcial o total del medio de comunicación.
- Pérdida de comunicaciones e información mientras viaja.
- Intercepción de información y comunicaciones (Man In The Middle).
- Suplantación o alteración de la información interceptada.
- Espionaje y monitoreo.

Medidas de prevención:

- Utilizar medios y herramientas de comunicación cifradas para:
  - Video y Voz
  - Chat o SMS
  - Envío y recepción de archivos
  - Navegación en Internet con servicios VPN y la red TOR.
- Verificar la autenticidad de la información a través de firma o huella digital, o de hashes.

Ataques digitales mediante

Conductas humanas

Implican abusar o aprovecharse del componente humano. En ocasiones involucran también una o varias vulneraciones técnicas.

Ataques digitales mediante conductas humanas

Como está descrito al inicio en la sección Aspectos a considerar; en esta categoría no incluimos **posibles riesgos**, ya que el impacto es de manera diferenciada, según quien ejerce los ataques, quien lo vive y en qué contexto social, cultural, económico, político tienen lugar. Por lo que al realizar un análisis de riesgo, es importante identificar otras vulneraciones según el contexto.

Las **medidas de prevención** incluyen acciones digitales. Para una prevención y atención integral, se deben incluir aspectos físicos, digitales y emocionales de acuerdo a cada caso.

Reiteramos que al utilizar esta tipología para documentar ataques digitales es clave tener en cuenta cómo se atacan grupos y comunidades específicas: por ejemplo mujeres y comunidades de diversidad sexual. Por lo que esta tipología tendrá que abordarse desde una perspectiva de género e interseccional.

Los ataques de esta categoría están divididos en **interacción directa e indirecta**.

- Los ataques vía directa son aquellos en los que la persona o grupo atacante establece contacto directo con la persona agredida a través de medios digitales, como mensajes en redes sociales, correos electrónicos, chats.

- Los ataques vía indirecta no implican una interacción, como cuando recaban información sobre una persona o grupo o una suplantación de identidad, por lo que suelen ser silenciosos o inadvertidos ya que la persona agredida puede no percatarse de qué está sucediendo.

Estos ataques pueden incluir contenido con fines de causar daño o desinformar, tales como: ofensas, contenido discriminatorio y de odio.

Interacciones directas

Conductas ofensivas o intimidatorias

Descripción:

Expresiones con el fin de ofender, avergonzar, asustar, humillar, desprestigiar, intimidar deliberadamente a otra persona. Los contenidos ofensivos pueden incluir amenazas, insultos y expresiones discriminatorias.

Ej. Memes ofensivos o imágenes deshumanizantes.

Conductas discriminatorias

Descripción:

Expresiones que reproducen la desigualdad, buscan otorgar un lugar inferior o insultar deliberadamente a personas o grupos en función de su género, origen étnico, rasgos físicos, religión, origen nacional, orientación sexual, discapacidad u otros rasgos.

Ej: Insultos relacionados al cuerpo, tatuajes, color de piel

Conductas que incitan al odio

Descripción:

Expresiones que incitan, amenazan o motivan a hacer daño con base en la identificación de una personas o grupo. También aquellas que incrementen un riesgo de violencia, motiven un ambiente de prejuicio y hostilidad, ataques o acciones perjudiciales.

Ej: Imágenes que afirman un ataque: “merece ser golpeada”

Los contenidos discursivos que incitan al odio odio no son libertad de expresión. Si la expresión incita a la violencia se considera conducta de odio.

Amenazas

Descripción:

Las amenazas anuncian un daño contra la integridad física y el bienestar de un grupo o persona. Con frecuencia incluyen expresiones ofensivas e intimidatorias. Las amenazas en línea no deben tomarse a la ligera, pues generan ansiedad, miedo y alteran el curso de la vida de una persona o grupo.

Ej: Mensajes amenazantes a través de chats, correos, llamadas: "sé donde vives, voy a buscarte".

Acoso

Descripción:

Son actos o comportamientos que fomentan un ambiente intimidante, hostil u ofensivo. Son indeseados para quien las recibe y tienen alguna o comparten estas tres características

a. Son intencionales

b. Si bien puede que no existe una subordinación, implican un desequilibrio de poder entre un agresor (individual o grupal) y una víctima

c. Son de naturaleza repetitiva y sostenida.

El acoso opera de manera horizontal entre personas de jerarquías homólogas o de parte de alguien que ocupa una posición menor a la de la persona acosada.

El acoso basado en el género está marcado por la intención de agredir a alguien en función de su género y orientación sexual.

Ej: "Te voy a seguir mensajeando hasta que respondas"

Hostigamiento

Descripción:
Son actos o comportamientos que fomentan un ambiente intimidante, hostil u ofensivo. Implican una manifestación de poder.

La relación subordinada en el hostigamiento, es la diferencia con el acoso.

Ej. “Mensajes molestos vía chats y que implican una relación laboral”

Extorsión

Descripción:
Implica amenazas, chantaje, intimidación con el fin de mantener control sobre una persona, grupo o entidad. Están relacionadas a publicar o distribuir información o contenido privado, sensible o íntimo. Y se puede pedir a cambio dinero, acciones contra la voluntad, o contenido íntimo y privado.

Ej: “Si no haces lo que te digo, publico tus fotos íntimas”

Medidas de prevención para ataques digitales de conducta humana por interacción directa

- Definir y gestionar perfiles o cuentas digitales según el tipo de información que contengan y su visibilidad.
- Separar o dividir información de acuerdo a cada perfil (público o privado)
- Configurar las opciones de privacidad de cuentas digitales, controlando qué información es visible y quiénes la pueden ver.
- Conocer las normas de comunidad y utilizar las opciones que incluyen las plataformas para dar de baja contenido ofensivo o intimidatorio (silenciar, bloquear o reportar). La respuesta de las plataformas dependerá del tipo de ataque.
- Dependiendo del contexto, contar con un registro de incidentes personal o colectivo (que contenga enlaces, capturas de pantallas y fechas) e incluir acciones y respuestas relacionadas.
- Contar con una red de apoyo que pueda responder ante la solicitud de aspecto físico, legal, digital, emocional.

Interacciones indirectas

Búsqueda y distribución sin consentimiento de información personal, privada, o considerada íntima *(doxing)*

Descripción:

Doxear es recopilar información personal o privada para posteriormente ser difundida en espacios públicos con el fin de atacar o dañar a una persona en específico. La información puede ser obtenida de distintas fuentes de acceso restringido, como son redes sociales personales, grupos de mensajería, correos electrónicos, etc. Comúnmente el doxing genera un ambiente de intimidación, acoso y amenaza, y puede escalar a acciones físicas de manera directa.

Este ataque también puede tomar la forma de divulgación de material gráfico y audiovisual explícitamente sexual o relacionado al rol de género, sin consentimiento y con el fin de causar daño.

Los ataques también pueden entrar en una dinámica de extorsión.

Ej. Una ex-pareja publica información íntima en redes sociales.

Ej. Un grupo opositor tiene acceso a información privada de una persona y publica esta información en redes sociales.

Medidas de prevención:

- Revisar la configuración de seguridad y privacidad de cuentas digitales y verificar qué información es pública.
- Revisar quiénes pueden ver información que es publicada en redes sociales.
- Realizar un “auto-stalkeo” para conocer qué tipo de información existe en internet sobre una persona. El auto-stalkeo consiste en buscar e identificar información publicada sobre uno misma(o), también incluye crear alertas asociadas a palabras clave a cerca de una persona o entidad para dar seguimiento de nuevos contenidos relacionados.
- Evaluar qué información personal podría ser usada para solicitar la baja de contenido de algún espacio digital.

Distribución de información (imágenes, audios, videos o datos) con fines de dañar o desinformar

Descripción:

Los intentos para desinformar y desprestigiar tienen lugar cuando una persona o grupos organizados publican en línea contenido negativo, falso, manipulado o sacado de contexto a través de grupos en redes sociales, en servicios de mensajería instantánea, sitios web o foros.

Este ataque puede tomar la forma de divulgación de material gráfico y audiovisual explícitamente sexual o relacionado a la actividad profesional de la persona con el fin de causar daño.

Ej. Un periodista que es despedido de un medio y posteriormente el medio publica contenido sacado de un contexto real que perjudica al periodista en su labor profesional.

Medidas de prevención:

- Contar con un grupo de apoyo para prevenir y atender situaciones de riesgo.
- Establecer y configurar alertas de contenido nuevo en Internet sobre tu persona, e.g alertas sobre contenido de Google

Suplantación y robo de identidad

Descripción:
La suplantación de identidad consiste en que alguien se haga pasar por una persona o entidad de manera maliciosa. Esto se puede lograr mediante la creación de perfiles falsos o contenidos en las redes sociales en nombre de alguien más sin necesidad de acceder a cuentas personales u oficiales.

El robo de identidad consiste cuando la suplantación escala y la identidad falsa comienza a identificarse como real o verídica, o mediante el robo de accesos (usuarios o contraseñas) de un perfil.

El robo y la suplantación de identidad suelen incluir:

- El acceso a información personal: nombre y apellidos, número de seguridad social, tarjeta de crédito, dirección física, correo electrónicos, teléfono, fotos, videos, contactos.
- La creación de cuentas, perfiles o contenidos falsos en redes sociales usando datos reales o falsos.

Ej: “Alguien se está haciendo pasar por mí en Facebook”

Medidas de prevención:

- Activar notificaciones en cuentas en línea para notar actividad extraña
- Cambiar contraseñas, en caso de notificación de intento de acceso a cuentas
- Revisar carpetas de correo enviado, basura y spam
- Activar la verificación de 2 pasos en cuentas en línea
- Poner atención a documentos que contienen información personal, manteniéndolos en lugares seguros.
- Documentar la actividad de las cuentas falsas y reportar a la plataforma que corresponda.
- Revisar las opciones de privacidad y seguridad de tus cuentas.

Vigilancia

Descripción:

Acecho e intromisiones reiteradas y obsesivas a una persona o grupo con el fin de dar seguimiento a sus actividades, obtener información privada o sensible y/o enviar información a alguien más.

Las prácticas de vigilancia pueden ser seguimiento de actividades en espacios físicos y digitales. Las más sofisticadas pueden incluir el uso de softwares maliciosos (malware) los cuales pueden adquirirse a través de la técnica phishing y que pueden tener funcionalidades como capturar contraseñas, copiar contenidos, grabar pantallas, activar y grabar audio y video.

Otro medio común para su realización es el uso de fuentes de información públicas en Internet como lo son redes sociales, foros, blogs.

Ej. “Recibí mensajes de números raros preguntando información personal.

Ej. También recibo solicitudes de amistad de perfiles desconocidos”

Medidas de prevención:

- Para prevenir la búsqueda de información y seguimiento de actividades en línea, sigue las acciones recomendadas en Doxing.
- Para evitar caer en engaños digitales que permitan acciones de vigilancia, sigue las acciones recomendadas en Phishing.
- Elige canales de comunicación segura que cuenten con cifrado de extremo a extremo.
- Usar un proxy para esquivar bloqueos a sitios web y contenidos. Un proxy es un servidor que sirve como intermediario para ocultar tu conexión y solicitudes en la web, manteniendo anónima tu identidad y la de tu equipo y redirigir el tráfico a otro país o zona geográfica para acceder a contenido censurado o restringido (Navegador Tor, VPN y DNS Alternativos).

Bloqueo o control de la distribución o publicación de información en plataformas, servicios o espacios digitales

Descripción:
Consiste en bloquear la generación, circulación o publicación de contenido por parte de proveedores de internet (ISP), plataformas digitales u organismos con poder en la toma de decisión sobre la información.

Ej. Que un ISP limite el acceso o conexión a servicios en específico brindando preferencia a estos servicios.

Ej. Que un ISP favorezca a una fuente de información en específico desfavoreciendo al resto de fuentes.

Ej. Una persona administradora de un espacio digital (como un sitio web) bloquea el acceso de publicación a una persona usuaria de manera arbitraria.

Medidas de prevención:

- Utiliza herramientas que aseguren tu privacidad mientras navegas, puedes utilizar el navegador Tor, una VPN o DNS alternativos.
- Elige canales de comunicación que cuenten con cifrado de extremo a extremo. El cifrado de punta a punta protege tu información mientras viaja en Internet.

Remoción de contenidos publicados en plataformas, servicios o espacios digitales

Descripción:

Consiste en remover o borrar contenido para evitar su disponibilidad, ya sea mediante reportes dirigidos a un contenido en específico desde plataformas, medios digitales, o a través de instrumentalizar vía legal una solicitud para remover contenido.

Ej. Una persona administradora de un espacio digital (como un sitio web) bloquea o elimina el contenido de una persona usuaria de manera arbitraria.

Medidas de prevención:

- Cuenta con un registro o documentación de publicaciones y contenidos en línea, esto podría incluir pantallazos o copias de los contenidos.
- Identifica redes de apoyo que puedan monitorear la remoción de contenidos y respuesta en caso de remoción y otras formas de censura.

Recursos finales

Herramientas de reporte en plataformas (2020)

Facebook

- Centro de Seguridad: https://www.facebook.com/safety
- Normas comunitarias: https://www.facebook.com/communitystandards/
- Herramientas: bloquear, dejar de seguir u ocultar personas y publicaciones; reportar.
    - Dejar de seguir: no verás sus publicaciones en tu News Feed, pero seguirás siendo amigo de ellos.
    - Bloquear: impide que la persona pueda agregarte como amigo y ver lo que compartes en tu biografía. *
    - Eliminar a la persona de tus amigos. Solo tus amigos de Facebook pueden ponerse en contacto contigo mediante el chat de Facebook o publicar en tu biografía
    - *Al tomar estas acciones, no se tendrá acceso a contenido futuro o
    - contenido previo publicado por esa persona.
    - Reportar una cuenta o los contenidos abusivos que publique. https://www.facebook.com/help/reportviolation
- Recuperar una cuenta vulnerada https://www.facebook.com/hacked
- Formulario de robo y suplantación de identidad: https://www.facebook.com/help/contact/295309487309948
- Reportar imágenes íntimas sin consentimiento: https://www.facebook.com/help/contact/567360146613371
- Centro de prevencíón de bullying para adolescentes, padres y educadores https://www.facebook.com/safety/bullying

Recursos finales

Herramientas de reporte en plataformas (2020)

Twitter

- Centro de ayuda sobre reglas comunitarias https://twitter.com/rules.
- Formulario de apelación y formularios directos para reportar violaciones a las Reglas de Twitter. help.twitter.com/forms.
- Herramientas: silenciar, bloquear y reportar
- Silenciar: Esta función oculta los tuits o notificaciones de
- otra persona sin que lo sepa.
- Bloquear: Al bloquear una cuenta en Twitter, impides interacciones. El bloqueo puede resultar útil para controlar las interacciones no deseadas (no te contacten, no vean tus tuits y no te sigan)
- Listas de cuentas bloqueadas: es posible importar listas de cuentas bloqueadas elaboradas por otra persona, exportar tu propia lista de cuentas bloqueadas para compartir con otra persona y manejar diversas listas de cuentas bloqueadas de manera independiente. Esto puede ser útil para aquellas personas que están recibiendo ataques vía interacción directa de un grupo de personas.
- Reportar: Al reportar, el contexto que se proporcione es muy importante. Apoya el reporte con contexto, evidencia (por ejemplo captura de pantalla) y otros incidentes relacionados. Es posible reportar una cuenta, una lista por contenido abusivo o perjudicial, un tweet o múltiples, y mensajes directos para solicitar que el contenido sea eliminado.
- Cualquier persona, puede reportar una violación de los términos de uso o de las reglas de Twitter. Sin embargo, en la medida de lo posible es importante que la persona víctima de la agresión reporte para recibir directamente la respuesta y recomendaciones.
- Alfabetismo y Seguridad Digital: Mejores Prácticas en el uso de Twitter
- Formulario de reporte relacionado a explotación sexual infantil https://help.twitter.com/forms/cse
- Formulario de reporte relacionado a robo o suplantación de identidad https://help.twitter.com/forms/impersonation
- Formulario de reporte relacionado a comportamiento abusivo y amenazas violentas: https://help.twitter.com/forms/abusiveuser
- Otros medios de contacto: gob@twitter.com y la cuenta de @TwitterSeguro

Recursos finales

Herramientas de reporte en plataformas (2020)

Instagram

- Reportar una cuenta de suplantación en Instagram https://help.instagram.com/contact/636276399721841

Chats

- WhatsApp: Puedes reportar un grupo de chat o un contacto https://faq.whatsapp.com/21197244/#Report
- Telegram: Puedes reportar contacto, grupo, canal desde las opciones del celular y stickers o bots enviando un correo a abuse@telegram.org e incluyendo enlace y @username a reportar.
- Signal: Puedes bloquear un número de teléfono, contacto o grupo.

Recursos sobre medidas de prevención

- https://protege.la/checklist-de-seguridad-digital-%e2%9c%85/
- https://protege.la/basicos-seguridad-digital/
- https://protege.la/proteger-cuentas-en-linea/
- https://protege.la/es-momento-de-elegir-contrasenas-nuevas-y-seguras/
- https://protege.la/ataques-en-linea/
- https://protege.la/que-hacer-si-te-roban-o-pierdes-el-celular/
- https://protege.la/sobre-phishing-y-otros-enganos-digitales/
- https://protege.la/acciones-para-evadir-la-censura-de-informacion-en-internet/
- https://protege.la/guia-sexting-seguro/

Sobre responsabilidad de las plataformas y autoridades

Actores con poder regulatorio deben proporcionar información accesible y útil en contextos de ataques digitales para combatir la violencia.

La omisión o falta de información y respuesta por parte de plataformas digitales y autoridades con poder regulatorio sobre herramientas y procesos para prevenir y actuar ante ataques digitales, contribuyen a normalizar y escalar la violencia, así como a la impunidad.

Fuentes consultadas:

- 13 formas de violencia relacionadas a la tecnología
- Kit de primeros auxilios digitales
- Redes sociales en perspectiva de género
- Infografía sobre acoso en línea (Trollbusters)
- Online abuse 101
- Understanding technology-related violence against women
- Hate speech explained - a toolkit
- Discurso de odio e incitación a la violencia hacia las personas LGBTI
- Ley General de acceso a las mujeres a una vida libre de violencia
- Without my consent
- Seguridad, protección y privacidad de Twitter
- Libres en línea: qué hacer en twitter
- Discurso de odio en LATAM
- Dangerous Speech
- Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial