Privacidad

Es probable que los contactos relacionados con la privacidad en línea caigan dentro de tres amplias categorías: guía de buenas prácticas de privacidad, temas relacionados con el abuso de la privacidad, y preocupaciones acerca de la "reputación digital" o la "huella digital".

Los contactos de buenas prácticas de privacidad incluyen a un niño en busca de consejos sobre cómo administrar su privacidad en línea. Por ejemplo, cómo elegir contraseñas, administrar perfiles en redes sociales, y así sucesivamente.

Contactos sobre abuso de la privacidad se van a relacionar con brechas de seguridad; por ejemplo, si ellos creen que alguien conoce su contraseña o si están recibiendo un contacto no solicitado.

Un niño también puede llamar con preocupaciones sobre su "huella digital" o su "reputación en línea"; por ejemplo, si este o un amigo ha compartido información o contenido de manera pública que se debería haber mantenido en privado, y tiene preocupaciones acerca de las consecuencias. Esto podría incluir compartir imágenes sexuales o "sexteo", o "pornografía de venganza":

- Sexteo (sexting): Material sexualmente explícito/desnudo/semidesnudo, propiciado por sí mismo(a)
- Pornografía de venganza: Material sexualmente explícito que se comparte públicamente en línea sin el consentimiento del individuo mostrado, a menudo subido por ex parejas con la intención de avergonzar o humillar a un individuo, enlazando el contenido a otro contenido en línea de la persona, como los perfiles de redes sociales.

CUANDO UN NIÑO HACE CONTACTO DIRECTAMENTE

Felicite al niño por establecer contacto y hacer preguntas; escuchando al niño será capaz de comprender mejor la razón del contacto del niño.

Utilice preguntas para comprender si el contacto se relaciona con "buenas prácticas" de privacidad, con un abuso de la privacidad, o con la reputación digital del niño.

Si el niño ha llamado en relación con preocupaciones serias sobre su reputación digital o un abuso de la privacidad, ofrezca reafirmación y un oído atento. Ellos pueden sentir una variedad de emociones: Amenazados, avergonzados o angustiados. Felicite al niño por establecer contacto y reconozca su valentía al hablar. Es vital asegurarle al joven que ha tomado la decisión correcta y que usted está ahí para escucharlo y ayudarlo. De igual manera es importante asegurarse de decirle que no es su culpa y que de ninguna manera se le va a reprochar.

Sea claro en cuanto a la confidencialidad que le está ofreciendo para que el niño sepa lo que puede pasar con la información que comparte. Por ejemplo, explique que cualquier cosa que le digan va a ser privada a menos que le diga algo que le haga pensar que se encuentra en peligro y usted sea capaz de conseguirle ayuda, en cuyo caso usted hablaría con él/ella acerca de lo que va a hacer.

Construya una relación y dele tiempo y espacio al niño para que se sincere aún más y proporcione más información. Recuerde reconocer el impacto emocional de lo que ha ocurrido, y tenga cuidado de no hacer conjeturas sobre la situación.

Brinde apoyo emocional. Además de reunir información sobre el origen del abuso o asunto de reputación digital, intente entender como el niño ha sido afectado emocionalmente para que pueda apoyarlos en eso y si es necesario escalarlo o protegerlos.

Por ejemplo, en los casos en donde la "huella digital" se usa para extorsionarlos, es necesario escalarlo (ver guía de sextorsión).

Las preguntas deben de ser claras y abiertas, por ejemplo:

- ¿Nos puede decir cuándo pasó esto?
- ¿Alguien te hizo amenazas? ¿Te han pedido que produzcas más imágenes?
- ¿Qué se ha compartido? ¿Con quién? ¿En qué dispositivos/redes sociales se ha estado compartiendo?

Trate de hacerles entender que aunque parezca el fin del mundo, no lo es. Hable sobre estrategias que los pueden poner en control nuevamente.

Si un niño no está dispuesto a hablar sobre detalles específicos durante el contacto, anímelos a que llamen de nuevo - dele tiempo y espacio.

Discuta las opciones prácticas que son relevantes para el contacto específico (ver abajo).

CUANDO UN PADRE / ENCARGADO HACE CONTACTO

Felicite al padre / encargado por el avance y buscar consejo.

Use preguntas para entender si el contacto se relaciona a "buenas prácticas" de privacidad, o a un abuso de privacidad o la reputación digital del niño, y adapte la respuesta según ello.

Para apoyar la discusión en buenas prácticas de privacidad con los padres / cuidadores, usted puede usar un marco de referencia desarrollado por O2 y NSPCC: Explore, Hable, Acuerde y Gestione.

Explore: Ayúdelos a entender lo que son datos personales.

- Sus hijos necesitan proteger sus datos personales, o podría terminar en las manos equivocadas. Sus datos personales pueden incluir su dirección, nombre completo, cumpleaños, número de teléfono y nombre de la escuela. Esta información puede ser toda usada para bullying, extorsión, acoso sexual infantil o robar su identidad.
- Cuando las personas preguntan detalles personales, no siempre puede parecer peligroso. Pero usted debe asegurarse que su hijo nunca comparta su información personal en línea. La gente no siempre es quien dice ser.

Hable: Ayúdelos a entender la importancia de tener conversaciones con sus hijos.

- Explique que cualquier cosa que se comparta en línea puede estar ahí por siempre, aunque lo eliminen. No hay forma de saber quién copio o compartió la información. Pídale a su hijo que piense qué podría pasar si la persona equivocada obtuviera su información. Déjelos considerar las consecuencias, es más probable que la lección quede de esa forma.
- Déjeles saber que usted está ahí para ayudarles si cualquier cosa sale mal. Usted no estará enojado ni sobreactuará.

Esté de acuerdo con: Ayúdelos a entender la importancia de definir reglas con sus hijos.

- Esté de acuerdo en qué sitios, aplicaciones y juegos son apropiados para su hijo. Si su hijo quiere usar un “chatroom”, asegúrese de que es moderado y que usted lo ha revisado personalmente.

Gestione: Ayude a su hijo a entender su huella digital.

- Haga una búsqueda en línea para el nombre, apodo, escuelas y direcciones de sus hijos. Revise la imagen resultante también. Esto le mostrará cuál información sobre ellos es pública. Si tiene cualquier preocupación, discuta los resultados con su hijo y ayúdele a editar su perfil para hacerlo más seguro.

Para llamadas reactivas sobre el abuso de privacidad o temas relacionados con la reputación digital del niño, usted debe ofrecer seguridad. Por ejemplo, es probable que un padre / cuidador sienta una gama de emociones si descubre que su hijo ha compartido imágenes / videos en línea desnudo o casi desnudo. Se pueden sentir enojados, confundidos, asustados y puede que se culpen a ellos mismos por lo que ha pasado. Lo importante es que ellos entiendan que no es culpa ni de ellos ni del niño y que no se les va a reprochar por lo que ha pasado.

Anime al padre a mantener la calma, a no juzgar y a evitar cualquier solución de pánico. En particular, aconseje a los padres a no quitarle al niño el acceso a Internet - la consecuencia más probable de tal acción sería que el niño deje de hablar con el padre sobre problemas futuros por miedo a que se le desconecte de su vida digital.

Converse con los padres sobre los consejos prácticos (ver más adelante) y recuérdeles que su línea de ayuda está disponible para que su hijo llame por apoyo- pero tome en cuenta que no podrá compartir el contenido de la llamada con el padre sin el consentimiento del niño.

GSMA HEAD OFFICE,
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, United Kingdom
Tel: +44 (0)207 356 0600

Es importante también que hable sobre el posible impacto emocional sobre el niño de la discriminación, esto le ayudará al padre a estar atento de las señales a tomar en cuenta, así como el enfoque de apoyo para su hijo. Pídale al padre que hable sobre:

- Cualquier cambio que haya notado en el comportamiento de su hijo.
- Si acaso tiene preocupaciones actuales o pasadas por la salud mental de su hijo.

La recopilación de esta información le ayudará a informarse sobre si es necesario referir esto a los servicios de apoyo que se pudieran requerir. Usted debe también asegurarse de que el padre está buscando cualquier cambio subsecuente en el comportamiento de su hijo, aunque no haya habido cambios visibles reportados por el padre a usted en esta etapa.

CONSEJOS PRÁCTICOS:

Tómese su tiempo con el niño / padre para explorar opciones prácticas que puedan ayudar al contexto específico que está siendo discutido.

Los pasos prácticos que pueden ser discutidos para mantener el control de la privacidad en línea incluyen lo siguiente:

- **Revise las políticas y configuraciones de privacidad** de páginas web / aplicaciones que usa.
- **Contraseñas.** Nunca comparta contraseñas. Si usted piensa que alguien conoce su contraseña, cámbiela, escoja una contraseña que no puede ser adivinada; use una contraseña diferente para los diferentes servicios y actividades.
- **Perfiles y compartir información.** Maneje activamente su configuración de perfiles para que su publicación sólo pueda ser vista por el grupo de amigos que escogió. Tenga en cuenta que cualquier cosa que publique puede aún ser copiada y compartida más allá del grupo que escogió. No comparta información en línea que podría hacerle vulnerable a contacto no deseado / inapropiado o robo de identidad (por ejemplo, dirección, correo, número de teléfono, fecha de nacimiento, etc.).
- **Amigos**. Considere las solicitudes de amistad cuidadosamente, ¿qué sabe realmente sobre esta persona que le ha contactado?
- **Nombre del usuario.** Los nombres de usuarios no deberían incluir nunca información personal (es decir, el año en que nacieron, dirección otro o su nombre completo).
- **Historial**. Elimine su historial de búsqueda y salga de las páginas web cuando está lejos de su computadora.
- **Use software antivirus** en sus dispositivos y manténgalos actualizados.
- **Revise que las páginas web estén protegidas.** B Antes de ingresar información personal como contraseñas o detalles de pago, revise el símbolo de candado después de la dirección web o "https" adelante de la dirección de la página web en su navegador.
- **Piense antes de hacer clic** – si recibe un mensaje de correo de un extraño, piense antes de hacer clic en él o un enlace o archivo adjunto - puede contener virus.
- **Cubra su cámara web** – si no la está usando, desconéctela, cubra el lente o apúntela a una pared vacía.
- **Bloqueo**. Use sus configuraciones de privacidad o herramientas de bloqueo para prevenir contacto no deseado.
- **Esté alerta para el posible robo de identidad**. Por ejemplo, si recibe facturas por cosas que usted no ha pedido o correos electrónicos de organizaciones no conocidas, puede ser que alguien esté usando su identidad. Cambie todas sus contraseñas, preguntas secretas y otra información que usted usa para identificarse o servicios en línea.

Para contenido que ya ha sido compartido y del que ahora se arrepiente, puede discutir las opciones con el niño. Por ejemplo,

- ¿Puede el niño editar o eliminar el contenido si él lo subió?
- Si alguien más lo subió, o el contenido que usted subió ha sido compartido por alguien más, ¿podría el niño pedir que lo eliminen? Discutan las formas en que el niño puede hacer la solicitud.
- ¿Hay beneficio en eliminar la cuenta en la cual se comparte el contenido, y configurar un nuevo perfil en dicha página web?

Si el tema se relaciona con el "sexting" o pérdida de control de imágenes sexuales autogeneradas / material en línea, sugiere que el niño/ padre contacte el centro de seguridad en el sitio de la red social así como cualquier servicio variable para que remuevan el contenido, como una línea directa de

GSMA HEAD OFFICE,
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, United Kingdom
Tel: +44 (0)207 356 0600

reporte de internet nacional. Si hay extorción, por favor refiérase a la guía de sextorsión.

Para temas relativos al contacto no deseado ver la guía de contacto no solicitado.

SEÑALES DE ALARMA:

- El niño revela que él / ella es el sujeto de las imágenes producidas por un par o adulto.
- El niño está expresando pensamientos suicidas, tiene intenciones de dañarse a sí mismo o trauma emocional.
- El niño ha sido amenazado o chantajeado.

En caso de que surjan asuntos graves durante su conversación, siga los procesos estándares de seguimiento para la intervención de las fuerzas de policiales, servicios de protección infantil, etc. según corresponda.

GSMA HEAD OFFICE,
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, United Kingdom
Tel: +44 (0)207 356 0600