Guía del correo electrónico para las personas sobrevivientes

El correo electrónico puede ser una forma conveniente de enviar un mensaje que puede incluir imágenes, documentos u otros archivos adjuntos. Puede enviar correos electrónicos a través de un navegador web, una aplicación o un software de correo electrónico. Muchas personas utilizan cuentas de correo electrónico gratuitas conectadas a cuentas en la nube como Gmail, Apple o Microsoft (también conocidas como Outlook o Hotmail), o a través de su lugar de trabajo o escuela. En su lugar de trabajo o escuela puede utilizar un proveedor como Gmail o Microsoft para las direcciones de correo electrónico del personal y los estudiantes, incluso si las direcciones de correo electrónico utilizan el propio nombre de la organización en lugar de "gmail.com" o "outlook.com".

¿Cómo podría utilizarse el correo electrónico en su contra?

Una persona agresora podría leer su correo electrónico si tiene acceso a su cuenta, si ha instalado un programa espía (spyware) en su teléfono o computadora o ha configurado su cuenta para reenviar secretamente los correos electrónicos a su cuenta propia.

Una persona agresora puede enviar mensajes acechantes por correo electrónico, ya sea en el propio mensaje o en cualquier archivo adjunto, o puede crear una cuenta de correo falsa para engañarle, de modo que usted abra los mensajes o para ocultar su propia identidad. También podrían implementar un *píxel de seguimiento* en los correos electrónicos que le envíen, lo que podría darles información acerca de si usted leyó el correo electrónico y su ubicación al momento de leerlo. Los píxeles de seguimiento pueden añadirse en los correos electrónicos mediante herramientas de marketing y ventas, o introduciendo un código a un correo electrónico manualmente; no es necesario que alguien tenga acceso físico a su dispositivo. La sección "Estrategias para contrarrestar el acoso por correo

electrónico" de este documento, habla de formas de abordar estas formas de acoso.

Dé prioridad a la seguridad

Utilice un dispositivo más seguro. Si sospecha que alguien está espiando su correo electrónico, utilice un dispositivo diferente o una cuenta a la que esa persona no pueda acceder (y a la que no haya tenido acceso en el pasado), como una computadora en una biblioteca o el teléfono de alguna amistad.

Obtenga más información. Atravesar una situación de violencia, abuso y acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a encontrar opciones y recursos locales y a crear un plan para su seguridad. Puede ponerse en contacto con una línea directa nacional para que le pongan en contacto con los servicios locales.

Estrategias generales de privacidad y seguridad del correo electrónico

- Cuando tenga que proporcionar información de carácter delicado o personal, evite utilizar el correo electrónico, sobre todo si la persona agresora puede tener acceso a la cuenta de correo o a los dispositivos utilizados para leer los correos.
- Procure no abrir los archivos adjuntos ni hacer clic en los enlaces que le envíe la persona agresora o alguien que no conozca. Pueden contener stalkerware u otro software dañino. Utilice una aplicación o software antivirus en su computadora, tableta y teléfono.
- Desactive la descarga automática de imágenes en sus correos electrónicos (porque las imágenes son una forma popular de enviar píxeles de seguimiento por correo electrónico). Este artículo se describe cómo hacerlo para Gmail, Outlook y Apple Mail.

- Lo que usted ponga en un mensaje de correo electrónico puede ser rastreado. Puede utilizar una herramienta de bloqueo de rastreadores de correo electrónico, como Trocker, que bloquea la capacidad de una persona de utilizar píxeles de rastreo para ver cómo responde a los correos electrónicos que ellos mismos envían. Esto les impide utilizar píxeles de seguimiento para conocer su dirección IP (ubicación geográfica general), la hora a la que lee un correo electrónico o la tecnología que utiliza para leerlos.
- Si necesita compartir documentos o fotos, utilice un sitio web para compartirlos.
- Puede obtener una nueva cuenta de correo electrónico que la persona agresora no conozca. Además de las opciones gratuitas mencionadas al principio de este recurso, puede considerar utilizar un servicio de correo electrónico más seguro como Proton Mail para sus correos más delicados.
    - Puede tener más de un correo electrónico y utilizar cada cuenta para fines determinados. Por ejemplo, puede utilizar una cuenta para operaciones bancarias o para su empleo y otra para citas por Internet.
    - No acceda a la nueva cuenta de correo electrónico a través de una computadora o dispositivo que esté siendo vigilado.
    - Utilice contraseñas seguras para las cuentas nuevas y guárdelas en un archivo de contraseñas. Lea para saber más sobre cómo hacerlo.
    - Considere la posibilidad de mantener la cuenta anterior para conservar las evidencias.
        - Si así lo hace, es posible que desee iniciar sesión en la cuenta antigua desde un dispositivo más seguro, de manera

que la otra persona no pueda entrar en la cuenta y borrar las evidencias.

Estrategias contra el acoso a través del correo electrónico.

- Si recibe amenazas o cualquier tipo de acoso por correo electrónico, puede conservar los mensajes.
  - Aunque puede resultar tentador borrar el mensaje, algunas de las mejores evidencias se encuentran en el correo electrónico original mismo. Conservar los correos electrónicos originales y documentar lo que está ocurriendo puede ser útil si el acoso continúa y decide emprender acciones legales en el futuro.
  - Si la persona agresora tiene acceso a su cuenta, es posible que desee reenviar una copia del mensaje a otra cuenta de correo electrónico en la que dicha persona no tenga acceso, en caso de que se elimine el original. Esta otra cuenta de correo sólo debe utilizarse para guardar los correos reenviados, para minimizar la posibilidad de que sea descubierta.
  - También puede imprimir copias de los correos electrónicos, sin embargo debe asegurarse de incluir el encabezado completo de dicho correo, que podrá encontrar siguiendo estas instrucciones.
- Puede bloquear una dirección de correo electrónico específica o configurar un filtro para que los mensajes vayan a una carpeta separada o a otra cuenta.

Financiado por la subvención US DOJ-OVW Número 15JOVW-21-GK-02216-MUMU. Las opiniones, hallazgos y conclusiones o recomendaciones

expresadas, son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.