LA SEGURIDAD CIBERNÉTICA
AL TRABAJAR DESDE CASA

Cuando trabaja de forma remota, es importante seguir las mismas recomendaciones de seguridad cibernética que si estuviera en la oficina. El FBI advierte que el número de delitos cibernéticos relacionados con el coronavirus ha aumentado[1], por lo que es importante mantenerse en guardia cuando se conecta desde casa.

Consejos de seguridad cibernética:

Utilice contraseñas seguras

Las contraseñas para las cuentas de WiFi y del trabajo deben ser únicas y difíciles de descifrar. Comience con una frase especial de al menos 12 caracteres. Incluya letras mayúsculas y minúsculas, números y caracteres especiales. Evite incluir información personal y no utilice la misma contraseña para todo.

Refuerce doblemente la seguridad

La autenticación multifactorial agrega a sus cuentas de trabajo una capa adicional de seguridad. Esta función requiere que confirme su identidad con otro dispositivo al iniciar sesión en un sitio nuevo. Considere también la posibilidad de solicitar una contraseña para las llamadas de videoconferencia en línea.

Las actualizaciones son importantes

Instale las últimas actualizaciones disponibles para todos sus dispositivos, programas y aplicaciones, ya que normalmente incluyen medidas de seguridad mejoradas. Siempre que sea posible, opte por las actualizaciones automáticas.

Considere una RPV

Si su empresa no utiliza una red privada virtual (RPV), considere la posibilidad de invertir en la suya propia. Este software protege su red para reducir el riesgo de un ataque informático. Entre los servicios más populares figuran NordVPN y ExpressVPN.

Mensaje nuevo

¡Cuidado con los mensajes de correos falsos!

Cc Bcc

Los piratas informáticos suelen dirigirse a sus víctimas primero con correos electrónicos falsos personalizados o mensajes de phishing. Antes de hacer nada:

Revise la dirección de correo electrónico del remitente: Puede parecer un mensaje de su banco o de un compañero de trabajo, pero una dirección de correo electrónico incorrecta o mal escrita indica que es falsa.

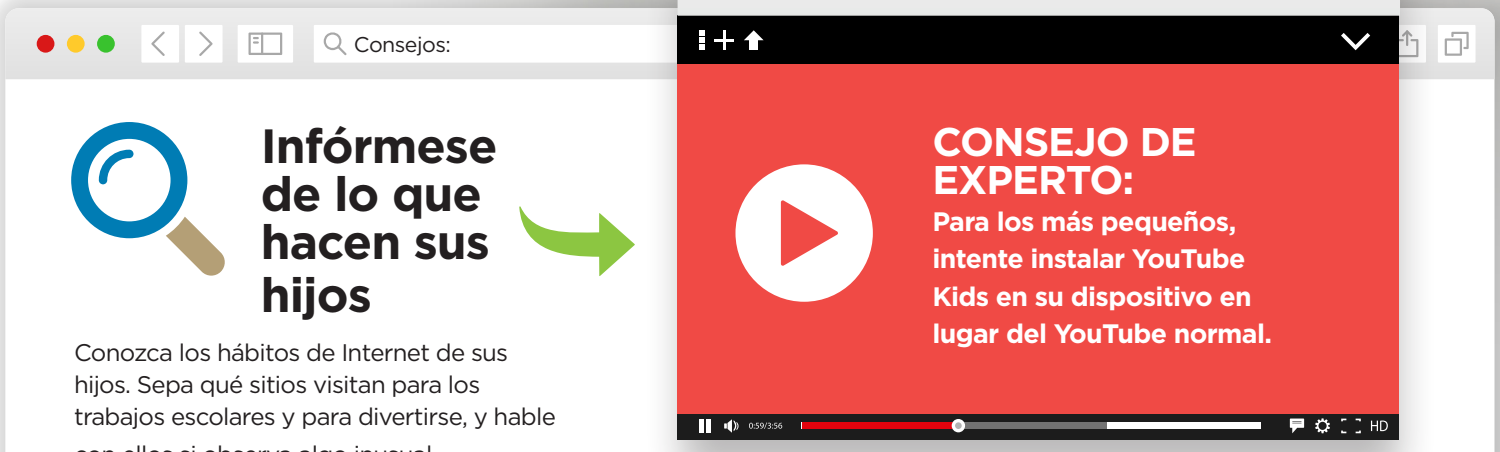
Desplácese por encima sin hacer clic: Coloque el cursor sobre el enlace para leer la URL. Si no puede reconocer el sitio es una señal clara de peligro, así que no haga clic en él.

Compruebe el tono: Los mensajes urgentes y atemorizantes que le exigen actuar de forma inmediata y con una fecha límite suelen ser falsos, incluso aunque parezcan venir de un compañero de trabajo.

Informe de la situación: Informe inmediatamente a su departamento de TI de la recepción del mensaje según el protocolo de la empresa.

CÓMO PROTEGER A SUS HIJOS EN LÍNEA

Ahora que las escuelas están adoptando el aprendizaje en línea y que las actividades al aire libre están limitadas, los niños pasan mucho más tiempo en línea. A continuación encontrará algunos consejos para asegurarse de que utilizan sus dispositivos de forma segura.



Infórmese de lo que hacen sus hijos

Conozca los hábitos de Internet de sus hijos. Sepa qué sitios visitan para los trabajos escolares y para divertirse, y hable con ellos si observa algo inusual.

Bloquee los sitios web peligrosos

Hable con su proveedor de Internet si desea bloquear ciertos sitios web de su red.

Establezca las reglas básicas

QUÉ HACER Y QUÉ NO HACER

Considere pedir a sus hijos que estén cerca cuando utilicen sus dispositivos y establezca reglas para los sitios que pueden visitar y cuándo, por ejemplo, YouTube sólo se permite fuera del horario escolar.

Fuentes: 1. FBI, "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic", 20 de marzo de 2020.