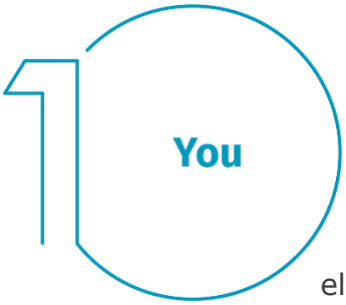
Los 5 pasos más importantes para trabajar desde casa de forma segura

Sabemos que trabajar desde casa puede ser una experiencia novedosa para muchos, y quizá la adaptación resulte un poco abrumadora. Uno de nuestros objetivos es ayudarle a trabajar desde casa de manera segura. Explicaremos cinco pasos para trabajar de forma segura. Lo mejor es que estas medidas no solo le ayudarán a salvaguardar su trabajo, sino que también protegerá sus datos y los de su familia creando un hogar ciberseguro.



Usted: Lo primero es que la tecnología por sí sola no puede protegerle. Usted es la mejor defensa. Los atacantes saben que la forma fácil de conseguir sus objetivos es ir a por usted, no lanzar ataques contra ordenadores o dispositivos. Si quieren conseguir su contraseña, sus datos de trabajo o el control de su ordenador, intentarán engañarle para que se los dé, a menudo creando una sensación de urgencia. Por ejemplo, quizá llamen haciéndose pasar por el servicio técnico de Microsoft y le aseguren que su ordenador está infectado. O puede que reciba un correo que dice que no han podido entregar un paquete, con el objetivo de que haga clic en un enlace malintencionado. Estos son algunos indicadores de los ataques de ingeniería social:

- Alguien intenta crear una gran sensación de urgencia, ya sea a través del miedo, la intimidación, una crisis o una fecha límite. A los ciberatacantes se les da bien crear mensajes convincentes que parecen de organizaciones de confianza, como bancos, organismos públicos u organizaciones internacionales.
- Presión para saltarse políticas o procedimientos de seguridad, o bien algo demasiado bueno para ser cierto (¡no, no ha ganado la lotería!).
- Un mensaje de un amigo o compañero de trabajo, pero con un tono o una forma de expresarse que no son los de esa persona.

Al final, usted es la mejor defensa contra estos ataques.

Red doméstica: Casi todas las redes domésticas parten de una red inalámbrica (a menudo llamada Wi-Fi). Es lo que permite que sus dispositivos se conecten a Internet. La mayoría de las redes inalámbricas domésticas se controlan desde un router de Internet o un punto de acceso inalámbrico independiente. En ambos casos, se transmiten señales inalámbricas a las que se conectan los dispositivos. Esto significa que proteger su red inalámbrica es esencial para proteger su hogar. Recomendamos llevar a cabo los pasos siguientes:

- Cambie la contraseña de administrador del dispositivo que controla la red inalámbrica. La cuenta de administrador permite modificar la configuración de la red.
- Asegúrese de que solo se puedan conectar personas de confianza. Implemente una seguridad sólida. En ese caso, hará falta una contraseña para que la gente pueda conectarse a su red inalámbrica y, una vez conectados, sus actividades en línea estarán cifradas.
- Asegúrese de que la contraseña que usa la gente para conectarse a su red inalámbrica sea segura y de que no coincida con la del administrador. Recuerde que solo será necesario introducir la contraseña una vez por dispositivo, ya que estos la almacenarán y la recordarán.

¿No tiene claro cómo proceder? Pregunte a su proveedor de servicios de Internet, consulte su sitio web y lea la documentación de su punto de acceso inalámbrico, o bien visite el sitio web del fabricante.

Contraseñas: Si un sitio le pide que cree una contraseña, use una sólida. Cuantos más caracteres tenga, más segura será. Las frases de acceso son la forma más sencilla de crear contraseñas sólidas. Una frase de acceso es una contraseña que consta de varias palabras, como "*abeja miel bourbon*". Emplear una frase de acceso única implica usar una diferente para cada dispositivo o cuenta en línea. Así, si una frase de acceso está en peligro, el resto de cuentas y dispositivos seguirán estando a salvo. ¿Le cuesta recordar todas sus frases de acceso?

Utilice un gestor de contraseñas, un programa especializado que las almacena todas en un formato cifrado (además de llevar a cabo muchas otras funciones útiles). Por último, siempre que pueda, active la verificación en dos pasos (o

autenticación de doble factor o multifactor). Este sistema emplea su contraseña, pero añade además un segundo paso, como un código enviado a su teléfono o una aplicación que genera un código. La verificación en dos pasos es quizá la medida más importante que puede tomar para proteger sus cuentas en línea y usarla es más fácil de lo que parece.

Actualizaciones: Todos sus ordenadores, dispositivos móviles, programas y aplicaciones deben emplear la última versión del software. Los ciberatacantes siempre buscan nuevas vulnerabilidades en el software que utilizan sus dispositivos. Cuando las descubren, emplean programas especiales para explotarlas y acceder a ellos sin permiso. Mientras tanto, las empresas que crean el software se esfuerzan por corregir el problema publicando actualizaciones. Si instala las actualizaciones cuanto antes en sus ordenadores y dispositivos móviles, será mucho más difícil que alguien acceda a ellos. Para estar al día, active las actualizaciones automáticas siempre que pueda. Esta regla es aplicable a casi cualquier tecnología de red, lo que incluye dispositivos de trabajo, televisores inteligentes, monitores para bebés, cámaras de seguridad, routers domésticos, consolas de videojuegos e incluso coches.

Niños e invitados: Algo que seguramente no le preocupa en la oficina es que haya niños, invitados u otros miembros de la familia que utilicen su portátil u otros dispositivos de trabajo. Explique a sus familiares y amigos que no pueden usar sus dispositivos de trabajo, ya que podrían borrar o modificar información involuntariamente, e incluso provocar infecciones de virus, lo que sería aún peor.