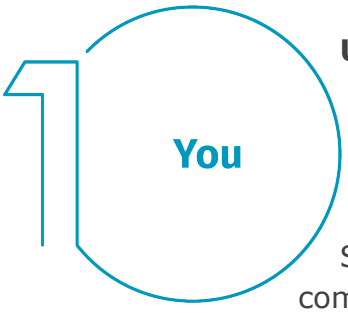
Los 5 pasos básicos para trabajar desde casa de forma segura

Sabemos que trabajar desde casa puede ser una experiencia nueva para algunas personas y, quizá, abrumadora mientras se adaptan al nuevo entorno. Uno de nuestros objetivos es permitirle trabajar desde casa de la forma más segura posible. A continuación, se enumeran cinco pasos simples para trabajar con seguridad. Lo mejor es que estos pasos no solo le ayudarán a incrementar la seguridad en su trabajo, sino que también le permitirán crear un hogar ciberseguro para usted y su familia.



Usted: ante todo, la tecnología no puede protegernos por sí sola, usted es la mejor defensa. Los atacantes han aprendido que la manera más fácil de obtener lo que buscan es que usted sea el objetivo de sus ataques, en lugar de centrarse en su computadora u otros dispositivos. Si quieren su contraseña, datos laborales o el control de su computadora, intentarán engañarle para que se los proporcione, a menudo por medio de una sensación de urgencia. Por ejemplo, pueden llamar fingiendo ser un empleado del servicio técnico de Microsoft y decirle que su computadora está infectada. O pueden enviarle un correo electrónico en el que le advierten que no fue posible entregar un paquete para que haga clic en un enlace malicioso. Los indicadores más comunes de un ataque de ingeniería social son los siguientes:

- Alguien crea una sensación de urgencia, recurre al miedo, intimidación, una crisis o una fecha de entrega importante. Los ciberatacantes son buenos creando mensajes convincentes que parecen de organizaciones de confianza, como bancos, organizaciones gubernamentales o internacionales.
- Le presionan para eludir o ignorar las políticas o procedimientos de seguridad o le hacen una oferta demasiado buena para ser real (no, no se ganó la lotería).
- Recibe un mensaje de parte de un amigo o colega, pero en el que la firma, el tono y el uso de palabras del mensaje hacen que no parezca escrito por esa persona.

En última instancia, usted es la mejor defensa contra estos ataques.

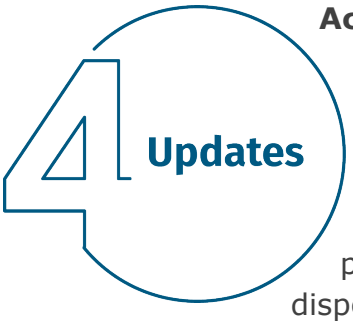
Red doméstica: prácticamente todas las redes domésticas comienzan con una red inalámbrica (a menudo, llamada Wi-Fi). Esta es la que permite que todos sus dispositivos se conecten a Internet. La mayoría de las redes inalámbricas domésticas están controladas por un router de Internet o un punto de acceso inalámbrico dedicado. Ambos funcionan del mismo modo, emiten señales inalámbricas a las que se conectan los dispositivos domésticos. Esto significa que garantizar la seguridad de su red inalámbrica es esencial para proteger su hogar. Le recomendamos seguir estos pasos para que sea segura:

- Cambie la contraseña predeterminada del administrador del dispositivo que controla la red inalámbrica. La cuenta de administrador es la que le permite definir la configuración de su red inalámbrica.
- Asegúrese que solo las personas de confianza puedan conectarse a su red inalámbrica. Para ello, se debe habilitar un nivel alto de seguridad. De este modo, se necesitará una contraseña para que las personas se conecten a su red inalámbrica y, una vez conectadas, sus actividades en línea estarán cifradas.
- Asegúrese que la contraseña que usan las personas para conectase a su red inalámbrica sea una segura y diferente de la contraseña de administrador. Recuerde que solo necesitará ingresar la contraseña una vez en cada uno de los dispositivos, dado que estos almacenarán y recordarán la contraseña.

¿No sabe cómo realizar estos pasos? Puede preguntarle a su proveedor de servicios de Internet, visitar su sitio web, consultar la documentación proporcionada con su punto de acceso inalámbrico o visitar el sitio web del proveedor.

Contraseñas: cuando le soliciten crear una contraseña en cualquier sitio, cree una segura. Cuantos más caracteres tenga, más segura será. El uso de una frase de contraseña es una de las formas más sencillas de crear contraseñas seguras. Una frase de contraseña es simplemente una contraseña que consta de varias palabras, como "*abejas-miel-whiskey*". Usar una frase de contraseña única significa usar una diferente para cada dispositivo o cuenta en línea. De este modo, si una frase de contraseña está en peligro, todas las demás cuentas y dispositivos se mantendrán seguros. ¿No recuerda todas sus frases de contraseña?

Use un administrador de contraseñas, que es un programa especializado que almacena de forma segura todas sus frases de contraseña en un formato cifrado (y, además, tiene muchas otras funciones interesantes). Por último, habilite la verificación en dos pasos (también llamada autentificación de dos factores), siempre que sea posible. Este método usa su contraseña, pero además, agrega un segundo paso, como un código que se envía a su smartphone o una aplicación que genera el código. La verificación en dos pasos es probablemente la medida más importante que puede implementar para proteger sus cuentas en línea, y es mucho más sencilla de que lo cree.



Actualizaciones: asegúrese de que sus computadoras, dispositivos móviles, programas y aplicaciones estén ejecutando la última versión del software. Los ciberatacantes buscan incesantemente nuevas vulnerabilidades en el software que usan sus dispositivos. Cuando descubren vulnerabilidades nuevas, usan programas especiales para aprovecharse de ellas y atacar los dispositivos que usted utiliza. Mientras tanto, las empresas que crearon el software de estos dispositivos trabajan arduamente para corregirlos a través del lanzamiento de actualizaciones. Al asegurarse de que sus computadoras y dispositivos móviles instalen estas actualizaciones de forma oportuna, logrará que sea mucho más difícil que alguien pueda atacarlos. Para estar al día, habilite las actualizaciones automáticas siempre que sea posible. Esta regla se aplica prácticamente a cualquier tecnología que esté conectada a una red, incluidos no solo los dispositivos de trabajo, sino también los televisores conectados a Internet, los monitores de bebés, las cámaras de seguridad, routers domésticos, consolas de videojuegos e, incluso, su automóvil.

Niños e invitados: seguramente en la oficina no tiene que preocuparse por que sus invitados, hijos u otros miembros de la familia utilicen su laptop de trabajo u otros dispositivos. Asegúrese de que sus familiares y amigos comprendan que no pueden usar sus dispositivos de trabajo, pues podrían borrar o modificar información accidentalmente o, aún peor, infectar el dispositivo sin querer.