

Cómo hacer que su organización sea segura dentro y fuera de la oficina

La seguridad de su organización debe ser una de sus principales prioridades, ya sea que trabaje desde su casa o en una oficina. Si bien esas dos ubicaciones pueden parecer diferentes, puede tener las mismas precauciones sin importar desde dónde trabaje. Veamos algunas reglas de ciberseguridad importantes y cómo pueden usarse en la oficina y cuando trabaja en casa.

Use solo dispositivos seguros

- Recuerde que su dispositivo es igual de seguro que las aplicaciones que se ejecutan en él. Nunca debe instalar una aplicación o un complemento sin consultar primero al departamento de TI.
- Solo use sus dispositivos de trabajo para trabajar. Si usa su computadora personal para trabajar, le recomendamos crear una cuenta de usuario diferente con un nombre de usuario y una contraseña únicos.
- Use una contraseña compleja en el router para proteger la conexión a Internet de su hogar. Si su organización ofrece acceso a una Red privada virtual (VPN, Virtual Private Network), conéctese a ella también.

Proteja su espacio de trabajo físico

- En la oficina, esté atento a la superposición de confirmaciones y al tailgating. Alguien que practica la superposición de confirmaciones es alguien que afirma ser parte de su organización y entra con usted a un área segura sin tener que usar una insignia o un código de entrada. Alguien que practica el tailgate es una persona que espera a que entre o salga de un área segura y se escabulle mientras la puerta sigue abierta. Sospeche de cualquier persona que no reconozca y no dude en pedirle su identificación.
- En su casa, busque un lugar de trabajo privado y cómodo, donde nadie pueda ver la pantalla mientras trabaja. Debe evitar que personas no autorizadas vean la información delicada, incluidos sus parejas, hijos y amigos.
- Bloquee siempre su computadora cuando se aleje del escritorio. Si la deja desbloqueada, cualquiera podría usarla para acceder a información delicada, robar sus credenciales de inicio de sesión o incluso instalar malware.

Piense antes de hacer clic

- Nunca descargue un archivo adjunto de un correo electrónico inesperado (ni haga clic en él). Aunque el remitente parezca ser parte de una organización legítima, la dirección de correo electrónico podría ser falsa.
- Cuando un correo electrónico le solicite iniciar sesión en una cuenta o en un servicio en línea, use su explorador para acceder al servicio. Nunca haga clic en el enlace del correo electrónico. Así se asegurará de estar iniciando sesión en el sitio web real y no en uno de apariencia similar.
- Si tiene dudas, llame al remitente del correo electrónico para asegurarse de que la solicitud, el enlace o el archivo adjunto sean legítimos. No llame al número de teléfono que figura en el correo electrónico, ya que podría ser falso.



El equipo de seguridad de KnowBe4