CYBERSECURITY AWARENESS MONTH

VÉASE USTED MISMO EN CIBER (SEE YOURSELF IN CYBER)

Todo el mundo tiene un rol en la ciberseguridad... no importa cuál sea su papel.

Cumpla su papel para que usted mismo y nuestra empresa permanezcan a salvo en cuanto a ciberseguridad emprendiendo cuatro acciones clave.

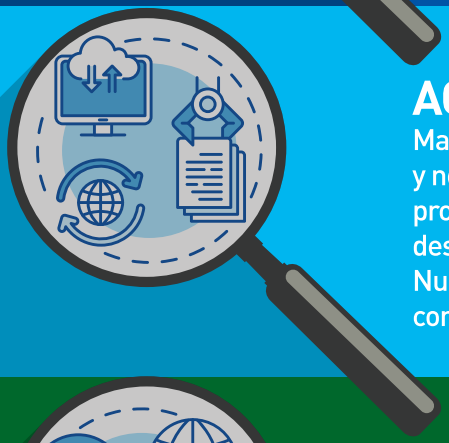
HABILITAR LA AUTENTICACIÓN DE FACTORES MÚLTIPLES

También conocida como autenticación de dos factores y verificación en dos pasos, la autenticación de factores múltiples es una medida de seguridad que exige que cualquier persona que inicie sesión en una cuenta navegue por un proceso de dos pasos para demostrar su identidad. Esto hace que sea el doble de difícil que los delincuentes accedan a una cuenta en línea. Al agregar un sencillo paso más al iniciar sesión en una cuenta, la autenticación de factores múltiples aumenta en gran medida la seguridad de su cuenta.

UTILICE CONTRASEÑAS SEGURAS

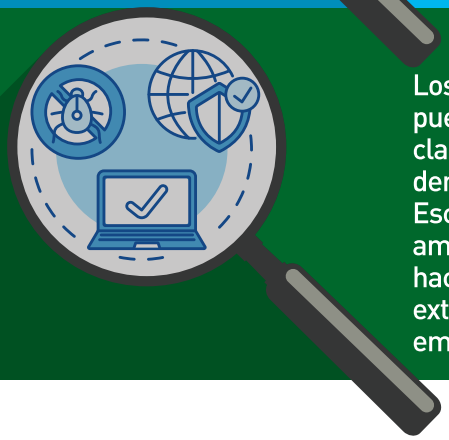
Las contraseñas son importantes si desea mantener su información segura. Aquí hay algunas formas sencillas de proteger sus cuentas a través de mejores prácticas de contraseñas. No importa cuál sea la cuenta, todas las contraseñas deben crearse con estas tres palabras en mente.

- Larga - Al menos 12 caracteres
- Única - Cada cuenta necesita su propia contraseña única
- Compleja - Utilice una combinación de letras en mayúsculas y en minúsculas, números y caracteres especiales. Algunos sitios web incluso le permitirán incluir espacios.



ACTUALICE EL SOFTWARE

Mantenga siempre su software actualizado cuando estén disponibles las actualizaciones y no se demore. Estas actualizaciones solucionan problemas generales del software y proporcionan nuevas revisiones de seguridad donde los delincuentes podrían entrar. Al descargar una actualización de software, solo obténgala de la compañía que lo creó. Nunca use versiones de software hackeadas, pirateadas o sin licencia, ya que a menudo contienen software maligno y causan más problemas de los que resuelven.



RECONOCER Y DENUNCIAR EL PHISHING

Los indicios pueden ser sutiles, pero, una vez que reconozca un intento de phishing, puede evitar caer en él. Éstos son algunos consejos rápidos sobre cómo detectar claramente un correo electrónico falso de phishing: Contiene una oferta que es demasiado buena para ser verdad, Lenguaje que es urgente, alarmante o amenazante; Escritura mal redactada con faltas de ortografía y mala gramática; Saludos que son ambiguos o muy genéricos; Solicitudes de envío de información personal; Urgencia para hacer clic en un hipervínculo o archivo adjunto desconocido; Solicitudes comerciales extrañas o abruptas; La dirección de correo electrónico de envío no coincide con la empresa de la que proviene.

MAUSER
Packaging Solutions