Proteja su empresa

Prácticas recomendadas para proteger su empresa de los fraudes

- Reconciliar sus cuentas bancarias todos los días.
- Efectúe los pagos de transferencias comunes y de ACH con control doble y autenticación de varios factores.
- Reporte todas las transacciones sospechosas de inmediato a Third Coast Bank SSB.
- Instale protección antivirus, malware y ransomware en todos los sistemas informáticos y recuerde actualizarla con regularidad.
- Instale con regularidad las actualizaciones para computadoras y servidores.
- Considere la posibilidad de emplear programas de detección de software espía.
- Verifique en el navegador que se establezca una sesión segura (https, no http) en todos los sitios de banca en línea.
- No utilice en la banca en línea opciones de inicio de sesión automático que guarden nombres de usuario y contraseñas.
- Mientras utilice un servicio de banca en línea, nunca se aleje de la computadora.
- Para las empresas que efectúan transacciones en línea, se recomienda realizar las actividades de banca en línea desde una computadora aislada, de seguridad reforzada y protección absoluta en la cual no se pueda utilizar correo electrónico ni navegar por Internet.
- Instale un firewall exclusivo.
- Cree copias de seguridad de sus datos con frecuencia.
- Sospeche de todos los mensajes de correo electrónico, en especial cuando se le pida una verificación de cuenta o se le soliciten credenciales de acceso a la banca, como el nombre de usuario, la contraseña, el NIP o datos similares. Al abrir archivos adjuntos o hacer clic en enlaces de mensajes sospechosos, podría exponerse a código malintencionado que tome el control de sus computadoras y sistemas.
- Cree una contraseña segura de al menos 8 caracteres y que combine minúsculas, mayúsculas, números y caracteres especiales.
- Utilice una contraseña diferente para cada sitio web.
- Conéctese únicamente a redes WIFI que tengan su absoluta confianza. Desactive la función de conexión automática en su dispositivo móvil.