EVITE EL FRAUDE

Hoja de Cálculo para Mostrar una Perspectiva de 360 Grados de los Negocios Pequeños

¿SE TRANSFIEREN SUS FONDOS DE FORMA SEGU	¿PIERDE GANANCIAS COMO CONSECUENCIA DE FR
¿MANTIENE LA INFORMACIÓN DE SU NEGOCIO PRIV	¿RECIBE E-MAILS SOSPECHOSOS Y ATENTADOS DE MA
¿ES CONSCIENTE DE LAS ÚLTIMAS TENDENCIAS DE	¿TIENE PROVEEDORES LEGÍTIMOS?
¿SON SUS CONTROLES INTERNOS SUFICIENTEMENTE	

EVITE EL FRAUDE

Lista Control de las Mejores Prácticas para Negocios Pequeños

FUNDAMENTOS FINANCIEROS DE REGIONS

PAGOS

1. Concilie para detectar actividad anormal.

- Concilie sus cuentas de manera oportuna.
- Categorice sus cuentas según propósito, tipo, y/o método de pago.

2

Para empleados

- Use Cámara de Compensación Automatizada (ACH).
- Si un empleado no tiene cuenta bancaria, deposite su pago en una tarjeta nómina que use como tarjeta de débito.

Para proveedores

- Pague vía ACH o tarjeta de compras.
- Haga transferencias electrónicas para pagos de alto valor o de tiempo delicado.

4

5. Use *Positive Pay*. Poderosa herramienta que le permite enviar información a su banco sobre los cheques que ha escrito para que cuando lleguen a pagar, coincidan con lo que usted les dijo. *Positive Pay* está disponible para ACH también.

Si usted ha autorizado a un proveedor u otro socio para que retire dinero de su cuenta, puede pre-aprobar la transacción.

BANCA POR INTERNET

1. Use control dual para iniciaciones de transacción.

- Use trasferencias electrónicas y ACH.
- Use alertas de email para aprobaciones.

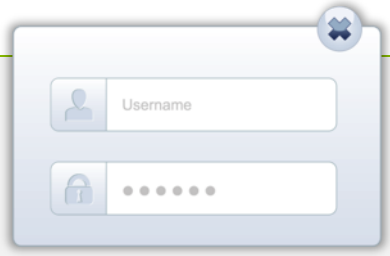
2 **Concilie sus cuentas diariamente para buscar actividad fraudulenta.**

- Use una computadora privada.
- Limite el uso de la internet
- Use programas de protección: firewall, anti-virus, anti-malware, anti-spyware.

4

Use CLAVES difíciles y protéjalas.

- Cree claves **difíciles de adivinar.**
- **Cambie su clave** al menos cada 60 días.



- **Mantenga sus claves seguras**. No tenga una lista de claves ni la mantenga cerca de su computadora. No comparta su clave o información de inicio de sesión con nadie.
- **Cuidado con la ingeniería social.** Sepa que el banco nunca lo llamará para preguntarle por su usuario ni por su clave.

- **No haga clic en links** que parezcan sospechosos.
- **Cuidado con estafas publicitarias para escáner de virus** que muestran lo que parece un escáner de virus de su computadora.
- **Nunca haga clic en Pop-Ups que digan que nuevo software debe ser instalado o comprado** para resolver problemas.
- **Cuidado con publicidad banner.** Son usadas por hackers para ocultar malware que puede ser instalado en una PC sin que el usuario haga clic en ellos.

RECURSOS

Regions:http://espanol.regions.com/commercial_banking/tms_protection.rf

Quejas de crimen en Internet:www.ic3.gov

Safe Checks Fraud Bulletin: http://www.safechecks.com/services/fraudbulletin.html

REGIONS