C4

DARC

B.E.C. (Business Email Compromise)

Se define como una estafa sofisticada, destinada a las empresas que trabajan con proveedores y/o con empresas donde se llevan a cabo los pagos a través de transferencias electrónicas nacionales e internacionales.

La estafa compromete cuentas de **correo electrónico corporativos** a través de técnicas de ingeniería social o del acceso a la información para llevar a cabo transferencias no autorizadas de fondos.

Delitos tipificados Ley 1273 de 2009:

- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Pena de prisión de 4 a 10 años.

VECTORES DE ATAQUE

- Uso de cuentas de correos falsos
- Falsos mensajes de chat en WhatsApp
- Falsos portales web
- Falsificación de documentos

Recomendaciones

Evitar compartir información en internet (uso adecuado en redes sociales).

El primer paso para evitar que un ataque BEC es no ceñirse a la comunicación por email.

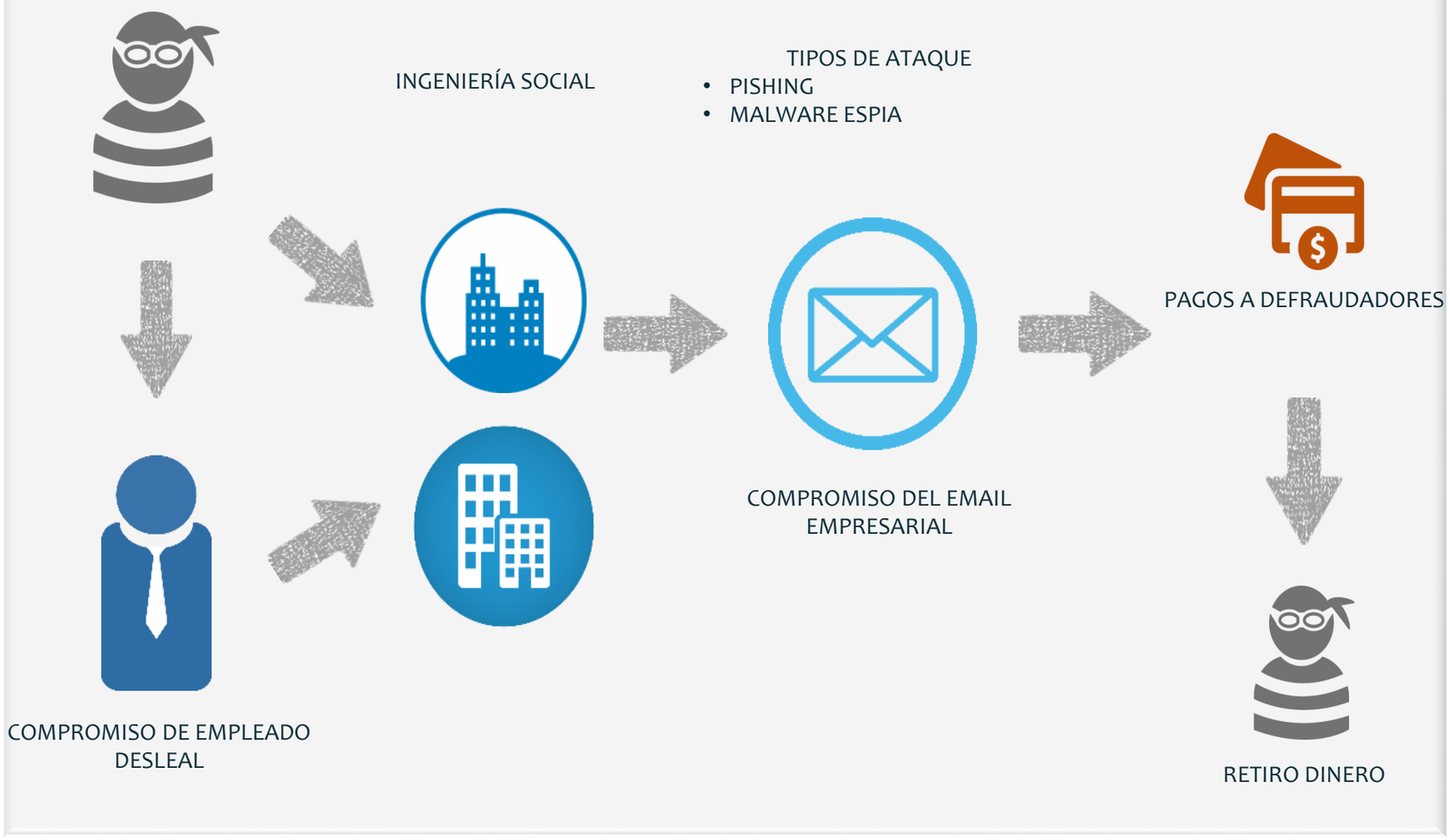
Establecer métodos de doble factor de autenticación por otros medios de comunicación.

Instalar soluciones de seguridad avanzadas que bloqueen el malware empleado para perpetrar los ataques BEC.

Es fundamental concienciar a los empleados de que de ellos depende en gran medida la seguridad de la empresa.

Validar cambios de cuentas corporativas de manera personal con proveedores y clientes.

Modalidad Criminal de Ataque B.E.C.



CARACTERISTICAS DEL ATAQUE BEC

- Un dominio de remitente falso
- Un asunto del correo electrónico urgente solicitando la transferencia de fondos inmediatos
- Cuerpo del correo electrónico
- Posición del remitente del correo electrónico