Hábitos sencillos que **protegen tu empresa de los ciberataques**

Las decisiones que toman a diario las personas, incluso las más pequeñas, pueden **abrir una puerta a los ataques cibernéticos dirigidos a generar afectación en la operación,** las finanzas y la reputación de la empresa. Para evitarlo, Fernando Olaya, gerente de Tecnología de la Cámara de Comercio de Cali y experto en protección de datos, comparte **hábitos simples** que tú y tu equipo pueden **aplicar de inmediato** para crear un verdadero **escudo digital,** sin necesidad de hacer más gastos.

Señales de alerta que debes detectar de inmediato

Cuando recibas un correo, un mensaje de texto o de WhatsApp, antes de realizar cualquier acción, revisa:

- **¿El remitente es extraño o muy parecido al oficial?**
  Una letra, un punto o un guión pueden cambiar toda la dirección. No es igual *ccc@ccc.org.co (la dirección oficial)* a *ccc@ccc.orgco* o *ccc@ccc.com.co*.
- **¿Tiene adjunto un archivo con un nombre capcioso?**
  Ten especial cuidado si contiene PDFs o archivos con las palabras "multas", "embargos", "actualización de datos", y otro tipo de solicitudes que suenan urgentes.
- **¿Incluye un enlace sospechoso?**
  Si dice "haz clic aquí" o solicita tu usuario y contraseña, evita seguir las instrucciones.
- **¿Busca provocar emociones fuertes?**
  Mensajes que generan miedo ("estás sancionado"), urgencia ("actualiza YA") o euforia ("te ganaste un premio") son tácticas aplicadas para que actúes por impulso.
- **¿Es un mensaje que no esperabas?**
  Si no tiene relación con asuntos de tu negocio, es mejor actuar con cautela.

Qué hacer si detectas un mensaje sospechoso

1. No abras enlaces ni descargues adjuntos.
2. Toma una captura de pantalla y envíala al área responsable de verificar.
3. Valida con la fuente oficial si ellos enviaron el mensaje.

Si ya realizaste alguna acción (descargar, abrir enlaces o ingresar datos):

1. Reporta de inmediato al área de tecnología o a tu proveedor de ciberseguridad.
2. Apaga el equipo afectado y desconéctalo de la red Wi-Fi.
3. Cambia tus contraseñas desde un dispositivo diferente.
4. Informa la situación al equipo de la empresa para evitar que otros caigan en la trampa.

Hábitos diarios que todo colaborador debe aplicar

Estas acciones simples reducen el riesgo de ser objeto de ciberataques:

- **Desconfía de lo "demasiado fácil" o "demasiado alarmante".**
  Lo gratis, rápido o inesperado suele ser la carnada del atacante.
- **Verifica siempre la fuente.**
  Revisa enlaces y direcciones antes de abrir, y confirma con el remitente real, con el área de tecnología o en canales oficiales.
- **Evita utilizar contraseñas repetidas o muy sencillas.**
  Es el error más común y aprovechado por los atacantes.
- **No compartas información privada o sensible por WhatsApp o mensajería instantánea.**
  Son útiles, pero no siempre seguras.
- **No uses redes Wi-Fi públicas para trámites sensibles.**
  Pueden ser redes falsas creadas para capturar información.
- **No conectes memorias USB desconocidas.**
  Aunque parezca "un acto de buena fe", es una vía común de infección o infiltración.

"Proteger la información corporativa y personal es tarea de todos. Un solo clic hace la diferencia. La mejor defensa contra los ciberataques es contar con un equipo consciente y con buenos hábitos de seguridad digital".

Fernando Olaya, gerente de Tecnología de la CCC, experto en protección de datos.

Fortalece las capacidades digitales de tu empresa

Si quieres profundizar en prácticas y conocimientos clave para **gestionar mejor la información** y **potenciar la eficiencia de tu negocio**, conoce la **Ruta de Transformación Digital Empresarial** de la Cámara de Comercio de Cali. Explórala e inscríbete aquí.

Cámara de Comercio de Cali