GESTIÓN

Siete acciones inmediatas para proteger tu farmacia de un ciberataque

POR BRUNO PEREZ JUNCA, PERITO INFORMÁTICO FORENSE, ESPECIALISTA EN CIBERSEGURIDAD, FORMADOR Y CONSULTOR, WWW.BRUNOPEREZJUNCA.COM

La mayoría de las farmacias creen que un ciberataque es algo lejano... hasta que un día no pueden acceder a recetas, pedidos o historiales.

La realidad es que las farmacias se han convertido en objetivos muy atractivos porque trabajan con datos sensibles, sistemas conectados y una operativa crítica donde cualquier interrupción genera un problema inmediato.

La buena noticia es que muchos ataques pueden evitarse aplicando medidas muy sencillas.

En este artículo veremos siete acciones prácticas que cualquier farmacia puede empezar a aplicar hoy mismo.

1. Activa hoy mismo el doble factor en WhatsApp y correo

Una contraseña robada no debería bastar para entrar en las cuentas de la farmacia. Sin embargo, muchos ataques actuales se producen precisamente porque los ciberdelincuentes consiguen acceder únicamente utilizando credenciales filtradas.

El doble factor de autenticación (2FA) añade una segunda barrera de seguridad. Aunque alguien conozca la contraseña, necesitará además un código adicional para acceder.

Es especialmente importante activarlo en:

- WhatsApp.
- Correo electrónico.
- Plataformas de gestión.
- Servicios *cloud.*

Acción inmediata

Entra hoy mismo en: Configuración → Cuenta →Verificación en dos pasos.

2. Crea una 'prueba de vida' interna

La inteligencia artificial ya permite clonar voces y generar conversaciones extremadamente creíbles. Esto significa que una llamada aparentemente legítima podría no serlo.

Por ello, resulta recomendable crear una pequeña 'prueba de vida' interna entre las personas de confianza de la farmacia. Puede tratarse de:

- Una palabra clave.
- Una frase acordada.
- Una pregunta cuya respuesta solo conozcan las partes legítimas.

No te olvides

Antes de facilitar información sensible o realizar pagos, verifica siempre la identidad utilizando esa palabra o frase acordada.

Hoy ya no basta con reconocer una voz.

3. Desconfía de cualquier urgencia

Los atacantes utilizan la presión psicológica para conseguir que las víctimas actúen sin pensar.

Correos de proveedores, mensajes bancarios o llamadas técnicas suelen incorporar frases como:

- 'Hazlo ahora'.
- 'Es urgente'.
- 'Último aviso'.

Regla básica

Nunca realicéis pagos, instaléis programas o facilitéis datos sin verificar antes la información utilizando otro canal de comunicación.
La urgencia es el mejor aliado del atacante.

4. Actualiza todos los dispositivos

Ordenadores, *tablets* y móviles forman parte de la seguridad de la farmacia. Muchos ataques aprovechan vulnerabilidades ya conocidas para las que existían actualizaciones disponibles.

Acción inmediata

- Activar actualizaciones automáticas.
- Revisar dispositivos antiguos.
- Mantener antivirus actualizados.

Actualizar no es comodidad, es protección.

5. Revisa quién tiene acceso a la farmacia

Muchas farmacias mantienen cuentas antiguas o usuarios compartidos. Esto dificulta el control y aumenta el riesgo de accesos indebidos.

Acción inmediata

- Revisar usuarios trimestralmente.
- Eliminar accesos innecesarios.
- Evitar compartir credenciales.

No siempre entra un atacante desconocido; a veces el problema es un acceso olvidado.

6. Comprueba las copias de seguridad

Tener una copia de seguridad no sirve de nada si nunca se ha probado.

Acción inmediata

- Verificar que realmente existen *backups*.
- Probar restauraciones.
- Mantener una copia desconectada.

La copia que no se prueba puede no existir.

7. Habla de ciberseguridad con el equipo

La ciberseguridad no depende únicamente del informático o del titular de la farmacia. Todo el equipo debe saber detectar mensajes sospechosos y entender cómo actuar.

Acción inmediata

Dedicar cinco minutos mensuales a hablar de:

- Correos sospechosos .
- Llamadas extrañas.
- Intentos de fraude recientes.

El ciberataque no empieza en el ordenador; empieza en una conversación.

5 SEÑALES DE UN MENSAJE SOSPECHOSO

1. Urgencia
2. Enlaces externos
3. Errores
4. Solicitud de códigos
5. Cambios bancarios

Conclusión

La mayoría de los ciberataques no se producen por técnicas extremadamente sofisticadas. En muchas ocasiones comienzan con pequeños errores cotidianos: una contraseña reutilizada, un clic impulsivo o una llamada aparentemente legítima.
Precisamente por ello, la mejor defensa sigue siendo la prevención, la verificación y la creación de hábitos de seguridad dentro del equipo.
La ciberseguridad ya no es únicamente una cuestión tecnológica. Hoy es una parte esencial de la protección y continuidad de cualquier farmacia. ✚

Sección coordinada por Juan Carlos Serra