Blinda tu negocio: **cómo prevenir ciberataques costosos**

El **phishing** es una de las principales **amenazas de ciberseguridad** para las empresas de todos los tamaños. Con un simple mensaje, correo o llamada **tu información y tu dinero** pueden estar en riesgo. Amadeo Medina, experto en ciberseguridad, te cuenta cómo **identificarlo, prevenirlo y responder** de forma efectiva para mantener tu negocio seguro.

¿Qué es el pishing y por qué es crítico?

El phishing es un tipo de **ciberataque** en el que el **delincuente** se hace pasar por una entidad legítima **para obtener información confidencial** como contraseñas o datos financieros.

Existen 8 modalidades frecuentes:

- **Por correo electrónico:** enlaces o archivos adjuntos maliciosos.
- **Spear phishing:** ataques personalizados dirigidos a altos cargos, que suelen terminar en la instalación de softwares maliciosos como el ransomware.
- **SMS phishing:** mensajes de texto con links que inducen a acciones peligrosas.
- **Voice phishing:** llamadas falsas para obtener contraseñas o clonar voces.
- **Pharming:** redirección a sitios web falsos para robar datos.
- **Phishing en redes sociales:** robo de cuentas para engañar a contactos.
- **Quishing:** uso de códigos QR con enlaces maliciosos.
- **Apps o plataformas falsas:** imitan servicios legítimos para instalar softwares maliciosos.

El **spear phishing** es el **más común y peligroso para las empresas**, pues los mensajes personalizados **generan confianza**, logrando que revelen datos sensibles o se instalen ransomwares que pueden **comprometer la operación y generar pérdidas significativas**.

Lo que está en juego con un ciberataque

El phishing puede costarle a tu negocio mucho más que dinero:

- Pérdida de datos críticos (inventario, CRM, contabilidad).
- Secuestro de información (de tu empresa y tus clientes) y cobro de rescates.
- Daño a la reputación al hacer ver tu negocio como poco seguro o confiable.
- Sanciones legales y regulatorias.

4 claves para prevenir el phishing en tu negocio

Protégete antes de que ocurra el ataque con herramientas como:

- **Autenticación multifactor (MFA)** en los accesos a cuentas o información crítica.
- **Capacitación continua** en ciberseguridad para todos los miembros de tu empresa.
- **Segmentación de redes y control de privilegios,** limitando los accesos a información crítica o datos sensibles según los perfiles y roles de cada colaborador.
- **Firewalls,** sistemas de seguridad que controlan y monitorean el tráfico de red.

Cómo identificar un ataque

- La detección temprana puede salvarte:
- Usa herramientas de **alertas** por comportamiento anómalo.
- Implementa **detección de phishing** en tiempo real para **correos electrónicos.**
- Incorpora **inteligencia de amenazas y monitoreo 24/7** (si es posible).

Buenas prácticas individuales:

- No abras links ni descargues archivos sin confirmar con el remitente.
- Guarda el mensaje sospechoso para la investigación forense.
- Verifica por llamada cualquier solicitud de pagos o transferencias.

Pasos inmediatos ante un incidente

Cuando detectas un eventual ataque:

1. Aísla el equipo o sistema comprometido.
2. Informa a TI o a tu proveedor de ciberseguridad.
3. Activa tu protocolo de respuesta a incidentes.
4. Conserva la evidencia (correo, mensaje, archivos).
5. Comunica a las áreas clave y afectadas.

Después del ataque:

- Restaura sistemas con copias de seguridad confiables.
- Identifica y cierra la brecha por donde entró el atacante.
- Informa a las personas o áreas afectadas.
- Realiza un análisis forense y refuerza la capacitación interna.

"No subestimen el riesgo, la clave está en la prevención más que en la reacción. Rodéense de aliados expertos, capaciten constantemente a su equipo y evalúen con frecuencia qué tan vulnerables son. Solo así podrán cerrar brechas antes de que ocurra un incidente".

Amadeo Medina, físico, criptógrafo y experto en ciberseguridad.

Cámara de Comercio de Cali

Ciberseguridad: tu ventaja competitiva

Bien gestionada, protege tu información, tu reputación y la continuidad de tu negocio.

En el programa **Mipymes Ciberseguras** de la Unión Europea y la Cámara de Comercio de Bogotá, en alianza con las Cámaras de Comercio de Cali, Barranquilla y Medellín, las empresas están aprendiendo a blindarse frente a amenazas como el phishing.

Fortalece también tu negocio con herramientas prácticas en la Ruta de Transformación Digital de la CCC.