

C18/CONV/2025 – Recomendaciones frente a las ciberamenazas

Con la llegada de la temporada navideña, se intensifica no solo la actividad comercial y de comunicación empresarial, sino también los riesgos de seguridad digital. Binaura Monlex colabora con CAEB para alertar sobre las ciberamenazas más relevantes en esta época y compartir recomendaciones prácticas para proteger tanto a empresas como a empleados y clientes.

💡 Principales amenazas detectadas este periodo**1. Incremento de dominios maliciosos y fraudes temáticos**

Durante los últimos meses se han registrado miles de dominios con temática navideña y de comercio electrónico, muchos de ellos con fines fraudulentos, utilizados para phishing, creación de tiendas falsas y robo de credenciales. Este tipo de infrae

2. structura maliciosa se aprovecha del aumento del tráfico y confianza del usuario en ofertas de temporada. [CISET. Centro de Innovación](#)**3. Estafas con tarjetas regalo y actividad comercial**

Los ciberdelincuentes están emitendo tarjetas regalo fraudulentas aprovechando la mayor actividad comercial de estas fechas, un truco que busca obtener datos financieros sin entregar valor real. [Europa Press](#)

4. Ataques de “Phishing 2.0” impulsados por IA

Los ataques de phishing han evolucionado notablemente: ya no son mensajes genéricos con errores evidentes. Ahora utilizan inteligencia artificial para crear correos electrónicos personalizados, convincentes y difíciles de distinguir de comunicaciones legítimas. Estos ataques suelen basarse en información pública o interna, y su objetivo es manipular al receptor con aparente confianza. [INCIBE](#)

5. Mayor sofisticación por uso de herramientas automatizadas e IA

Herramientas de IA facilitan la creación de correos fraudulentos, sitios web clonados y campañas de ingeniería social que se adaptan al estilo corporativo de destinatarios específicos. [El País](#)

❖ ¿Qué riesgos supone esto para nuestras organizaciones?

- Robo de credenciales y cuentas corporativas
- Exposición de datos sensibles (clientes y empleados)
- Fraude financiero a través de transacciones y compras no autorizadas
- Daños reputacionales y pérdida de confianza de clientes y partners

 **Recomendaciones clave para mitigar riesgos**

Para reforzar la seguridad y protección de datos en estas fechas, se aconseja:

- ✓ Activar autenticación multifactor (MFA) en accesos críticos.
- ✓ Verificar URLs y remitentes antes de introducir credenciales o datos sensibles.
- ✓ Aumentar la formación y concienciación del personal, especialmente sobre correos personalizados fraudulentos.
- ✓ Mantener actualizados sistemas, plugins y plataformas de comercio electrónico.
- ✓ Establecer controles en redes sociales y campañas digitales para evitar la suplantación de identidad de nuestra marca.
- ✓ Monitorizar actividad inusual en cuentas corporativas y canales de comunicación.

 La temporada navideña —con su aumento de transacciones, comunicaciones festivas y compras online— representa un terreno fértil para los atacantes. Una estrategia preventiva y de concienciación puede marcar la diferencia entre una campaña segura o una brecha con consecuencias económicas y reputacionales.

Desde Binaura – Grupo Monlex, están a disposición de las empresas para profundizar en medidas de protección específicas o apoyarles en la evaluación y mejora de su postura de ciberseguridad.

Más información y consultas: info@binauramonlex.com / <https://www.binaura.es>