Seguridad Digital

Navidad conectada, riesgos aumentados: la otra cara de la seguridad digital durante eventos y actividades sociales.

En la temporada navideña, las celebraciones presenciales se combinan con hábitos digitales de riesgo que facilitan fraudes, suplantaciones e intrusiones informáticas. La época navideña es sinónimo de fiestas, convivios, actividades públicas y movimiento masivo en redes sociales. Sin embargo, esta combinación genera un escenario digital altamente vulnerable. Durante diciembre, aumentan los casos de phishing, suplantación de identidad, robo de información y fraudes relacionados con promociones falsas y eventos masivos. La Criminología advierte sobre el riesgo de publicar información personal o de ubicación en tiempo real durante actividades sociales y eventos públicos. Lo que empieza como una celebración puede terminar convirtiéndose en una puerta abierta al delito digital.

Cuando la celebración se vuelve exposición, la criminología contemporánea reconoce que el espacio digital es hoy un entorno delictivo tan activo como el espacio físico. En la época navideña, se produce una convergencia peligrosa:

- Mayor tráfico en redes sociales,
- Aumento en compras y transacciones digitales,
- Incremento en publicaciones de fotos, eventos y ubicaciones,
- Sobreexposición emocional, típica de épocas festivas.

Desde la perspectiva de la criminología digital, cada publicación genera datos que pueden ser explotados por delincuentes informáticos. La rutina navideña, eventos, compras y ocio,

se traduce en rutinas digitales predecibles, que amplifican la exposición y reducen el autocontrol.

"La Navidad es celebrada en familia, pero compartida ante miles de desconocidos"

Los riesgos digitales durante actividades sociales son varios comportamientos que incrementan la vulnerabilidad:

1. Compartir fotografías y ubicación en tiempo real: Publicar desde un convivio, un bar, un concierto o un centro comercial informa al delincuente dónde se encuentra la persona y, más importante, dónde no está (su hogar).

"Esto abre puertas al robo, seguimiento digital o ingeniería social"

2. Conectarse a redes Wi-Fi públicas sin verificación: Muchos eventos navideños, ferias, conciertos, parques temáticos, ofrecen Wi-Fi gratuito. Estas redes son ideales para ataques Man-in-the-Middle, robo de contraseñas y suplantación de sitios web.

3. Interactuar con promociones, rifas o "regalos navideños" sospechosos: La temporada incrementa la emocionalidad y reduce el análisis crítico. Esto abre la puerta a estafas digitales camufladas como:

- Rifas navideñas.
- Cupones falsos.
- Enlaces de "solo por hoy".
- Perfiles falsos de comercios.

"Los datos del archivo muestran que estos engaños aumentan significativamente en diciembre"

4. Uso excesivo de redes sociales durante eventos: La distracción digital reduce la percepción situacional tanto física como cibernética. El usuario se desatiende y cae fácilmente en engaños, enlaces maliciosos o revelaciones involuntarias de información.

> ***"La Navidad no solo se vive: también se publica. Y ahí nacen los riesgos"***

Desde la criminología digital en entornos festivos se debe de comprender que la época navideña crea un ambiente emocional y social que la criminología considera un contexto facilitador del delito digital:

A. **Comportamientos más impulsivos:** La emoción festiva baja la guardia y aumenta la confianza en enlaces y ofertas.
B. **Rutinas digitales más activas:** Más fotos, más publicaciones, más interacción, es igual a más exposición.
C. **Delincuentes más activos y creativos:** Los ciberdelincuentes aprovechan campañas masivas, picos de consumo y el deseo de aprovechar "promociones navideñas".

La criminología ambiental aplicada al entorno digital señala que los delitos tecnológicos surgen cuando **convergen motivación del atacante, vulnerabilidad del usuario y ausencia de protección técnica.**

> ***"En diciembre, esas tres condiciones crecen simultáneamente"***

La seguridad digital en la época navideña no depende únicamente de antivirus, contraseñas o dispositivos seguros. Depende, sobre todo, de decisiones conscientes en momentos de alta emoción y celebración. Cada foto compartida, cada ubicación publicada y cada enlace abierto construyen un mapa de nuestra vida para quien busca explotarlo.

La Navidad es un tiempo para compartir, pero no para exponerse, la invitación es clara y urgente:

	No publiques tu ubicación en tiempo real
	Verifica redes, enlaces y promociones antes de interactuar
	Cuida tu información cómo cuidas a tu familia
✕	No te conectes a Wi-Fi públicos de origen dudoso

Fuente: Elaboración propia, 2025

Pero más allá de las medidas individuales, la prevención digital requiere un cambio cultural. Debemos entender que nuestra identidad digital vale tanto cómo nuestra seguridad física, y que la información compartida sin criterio se convierte en herramienta para el delito. El desafío no es dejar de celebrar; es celebrar con conciencia. Porque en Navidad, más que nunca:

> ***"La seguridad digital también es un acto de amor propio y de protección hacia los nuestros"***

Fuentes Bibliográficas

Clarke, R. V., & Newman, G. (2005). *Outsmarting the Terrorists*. Praeger.

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2018). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Ministerio de Seguridad Pública. (2024). *Recomendaciones de prevención para temporada navideña en entornos digitales*. Costa Rica.

0.2 Segundo Bloque de Tips (CR …

Yar, M. (2013). *Cybercrime and Society*. Sage Publications.