



INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 9



15 DE NOVIEMBRE DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

¿Qué es el Antifraude?	2
Tipos de Antifraude	2
Recomendaciones	2
Escenario de aplicación.....	3

¿Qué es el Antifraude?

Las soluciones Anti-Fraude están destinadas a proteger a los usuarios de todo tipo de ingeniería social. Uno de los objetivos de la ingeniería social es realizar actividades fraudulentas en internet, como el robo de información personal o datos bancarios, suplantación de identidad y otras. Todas ellas llevadas a cabo mediante técnicas como el phishing, el correo electrónico no deseado (spam) o el malware diseñado al efecto. El fraude on-line es una amenaza de amplio espectro, puesto que hace uso de múltiples técnicas, vías de entrada, servicios en internet o malware, pero sobre todo se basa en explotar la confianza de los usuarios, en base a la dificultad que tienen estos en diferenciar aquello que es legítimo de lo que no lo es.

Tipos de Antifraude

- Anti-phishing

Protegen del fraude iniciado a través del correo electrónico. Son comunicaciones destinadas a engañar a un usuario para conectar a un servicio fraudulento con el fin de obtener información de pago o credenciales de acceso al servicio legítimo.

- Anti-spam

Son herramientas destinadas a filtrar el correo electrónico no deseado, también llamado correo basura.

- Herramientas de filtrado de navegación

Son herramientas destinadas a proteger al usuario durante la navegación en internet, controlando los sitios a los que se accede mediante listas, reputación u otras.

- UTM, Appliance (Unified Threat Management)

Gestión Unificada de Amenazas, son dispositivos de seguridad en forma de Appliance que proporcionan varias funciones de seguridad en un único dispositivo.

Recomendaciones

- Usar los certificados digitales que nuestra página web o tienda online utilice en el protocolo https con un certificado emitido por una entidad de confianza;

- Implementar medios de pago que nos protejan en la medida de lo posible contra el fraude.

- Realizar comprobaciones sobre los pedidos, de modo que podamos mitigar en la medida de lo posible la gestión y envío de un pedido fraudulento.

- Concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen software sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa.
- Detectar posibles copias o usos no autorizados de las marcas o distintivos comerciales.
- Proteger las cuentas con contraseñas complejas. cambiar las claves de manera periódica.

Escenario de aplicación

Son productos destinados a la protección general contra el fraude on-line, mejorando enormemente la seguridad en todo tipo de transacciones electrónicas, pero también en el uso diario de Internet, con servicios habituales como el correo electrónico, los portales web, o la mensajería instantánea. Son herramientas con un ámbito de utilización muy amplio, desde la protección de un puesto de trabajo, hasta la seguridad de aplicaciones, sistemas y redes.