RIESGOS QUE CONLLEVA CONECTARSE A INTERNET

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

PLEXTEL COMUNICACIONES S.A.S.

Teniendo en cuenta la importancia que tiene para nosotros la seguridad de nuestros clientes, mediante este documento informamos las modalidades más comunes de vulneración al servicio de internet, a sus dispositivos, redes locales e información personal, así como las buenas prácticas recomendadas para su mitigación:

1. PHISHING (SUPLANTACIÓN DE IDENTIDAD)

Definición:

El *phishing* es una modalidad de estafa diseñada con la finalidad de apropiarse o robar la identidad del usuario. Este acto delictivo consiste en obtener información confidencial (claves de banca en línea, números de tarjetas de crédito, tokens de seguridad, contraseñas o datos personales) mediante engaños. Este fraude se recibe habitualmente a través de correos electrónicos, mensajes de texto (SMS / *Smishing*), llamadas telefónicas (*Vishing*) o ventanas emergentes (*pop-ups*).

Cómo funciona:

El delincuente envía masivamente mensajes falsos diseñados para aparentar que provienen de entidades oficiales o de su entera confianza (bancos, plataformas de comercio electrónico, empresas de mensajería, servicios públicos o autoridades gubernamentales). Incluyen enlaces falsos que redirigen al usuario a páginas web clonadas donde, al ingresar sus credenciales, la información es capturada para cometer fraudes financieros o robo de identidad.

Cómo protegerse:

La seguridad es una responsabilidad compartida entre **PLEXTEL COMUNICACIONES S.A.S.** y el usuario final. Se recomienda:

- Nunca responda a solicitudes de información personal o financiera enviadas por correo electrónico, mensajería instantánea o llamadas no solicitadas.
- Tenga especial cuidado con mensajes de plataformas de compra en línea (*Amazon, Mercado Libre, Temu, AliExpress, Shopee, eBay, PayPal*) o entidades financieras.
- Verifique remitentes y evite ingresar a enlaces para actualizar datos si no ha realizado dicha solicitud previamente.
- Asegúrese de que sus dispositivos (celulares, computadores, *tablets*) cuenten con el sistema operativo actualizado y una solución de antivirus activa.
- Digite directamente la dirección URL en la barra de navegación en lugar de hacer clic en enlaces recibidos.
- Compruebe que el sitio web utilice protocolos de conexión segura (https://) y presente el ícono del candado de seguridad en la barra del navegador.
- En caso de administrar servidores o dispositivos de red, mantenga actualizados los sistemas operativos y aplicativos conforme a las recomendaciones del fabricante.
- Reporte cualquier incidente de ciberseguridad a la Policía Nacional (CAI Virtual: caivirtual.policia.gov.co), a la Fiscalía General de la Nación y a **PLEXTEL COMUNICACIONES S.A.S.**

2. SPAM (CORREO BASURA Y MENSAJERÍA MASIVA)

Definición:

Se denomina *spam* a todos aquellos mensajes no solicitados (habitualmente publicitarios o con fines maliciosos) enviados de forma masiva por personas o bots no identificados. Además de saturar el buzón de entrada y la capacidad de almacenamiento, el *spam* suele utilizarse como vehículo para propagar código malicioso (*malware*) o enlaces de *phishing*.

Mitigación y acciones del usuario:

PLEXTEL COMUNICACIONES S.A.S. implementa filtros de red y bloqueos a direcciones IP reportadas por el envío de *spam*. No obstante, el usuario debe seguir estas recomendaciones:

- Si no reconoce al remitente de un mensaje, no lo abra ni descargue sus archivos adjuntos.
- Configure filtros anti-spam en su proveedor de correo electrónico.
- Clasifique como *spam* o correo no deseado cualquier mensaje no solicitado de origen dudoso.
- No ingrese a enlaces (*links*) dentro de correos de remitentes desconocidos.
- Evite registrar su dirección de correo en sitios web no confiables o de origen inseguro.
- Para verificar si un dominio o correo está en listas negras, puede consultar servicios públicos como www.dnsstuff.com o www.spamhaus.org.
- En caso de que su dirección IP pública sea reportada en listas negras debido a infecciones en sus equipos locales, proceda con la desinfección de la red e inicie el trámite de desbloqueo mediante los formularios oficiales de cada proveedor de reputación (ej. *Spamhaus, Barracuda, UCEPROTECT*).

3. VIRUS Y CÓDIGO MALICIOSO (MALWARE)

Definición:

Un virus o *malware* es un software diseñado para filtrarse, copiarse o ejecutarse en un dispositivo sin el consentimiento del usuario. Su objetivo es alterar el normal funcionamiento del equipo, alterar o destruir archivos, robar credenciales o permitir el control remoto no autorizado del dispositivo.

Cómo protegerse:

PLEXTEL COMUNICACIONES S.A.S. aplica políticas de seguridad en la red para bloquear la propagación de amenazas conocidas; sin embargo, el usuario debe adoptar las siguientes medidas:

- No abra ni ejecute archivos adjuntos de correos electrónicos de procedencia dudosa, aun cuando cuente con antivirus.
- Evite instalar software pirata, programas de descarga P2P no verificados o aplicaciones fuera de las tiendas oficiales (*Google Play Store*, *App Store*, *Microsoft Store*).
- Mantenga actualizado el sistema operativo (Windows, macOS, Android, iOS) y las aplicaciones instaladas.
- Instale y mantenga actualizado un software antivirus/anti-malware de fabricantes reconocidos.

4. RANSOMWARE (SECUESTRO DE INFORMACIÓN)

Definición:

El *Ransomware* es una de las amenazas más críticas en la actualidad. Es un tipo de *malware* que cifra (bloquea) los archivos del usuario o del sistema e impide el acceso a ellos, exigiendo posteriormente el pago de un rescate económico (habitualmente en criptomonedas) para entregar la clave de descifrado.

Cómo funciona:

Ingresa al dispositivo a través de adjuntos en correos falsos, descargas de programas no autorizados, archivos comprimidos o vulnerabilidades en sistemas no actualizados. Una vez ejecutado, inhabilita documentos de texto, fotografías, bases de datos o archivos de trabajo en cuestión de minutos.

Medidas de prevención:

- **Copias de seguridad (Backups):** Realice respaldos periódicos de su información importante en discos duros externos (desconectados de la red) o en servicios de almacenamiento en la nube seguros.
- Mantenga deshabilitada la ejecución automática de macros en documentos de Word o Excel recibidos por correo.
- Bajo ninguna circunstancia realice pagos por el rescate de la información, ya que esto no garantiza la recuperación de los datos y financia actividades delictivas.

5. INGENIERÍA SOCIAL Y SUPLANTACIÓN EN REDES SOCIALES Y MENSAJERÍA (WHATSAPP / TELEGRAM)

Definición:

Mecanismo de manipulación psicológica mediante el cual los ciberdelincuentes engañan a las personas para que entreguen voluntariamente información confidencial, accesos o dinero, o bien para tomar el control de sus cuentas de mensajería (ej. robos de cuenta de WhatsApp mediante el código de verificación).

Modalidades comunes:

- **Robo de cuenta de WhatsApp:** Solicitud engañosa del código de verificación de 6 dígitos bajo excusas de falsos premios, entregas de paquetes o soporte técnico.
- **Falsas ofertas de empleo o préstamos:** Mensajes que prometen ingresos altos por realizar tareas sencillas o préstamos de dinero inmediatos para captar datos financieros.
- **Suplantación de familiares:** Mensajes de números desconocidos asegurando ser un familiar con una emergencia económica.

Medidas de prevención:

- **Verificación en dos pasos:** Active la verificación en dos pasos en WhatsApp, Telegram, correo electrónico y redes sociales.
- **Código de confirmación secreto:** Nunca comparta con nadie el código de verificación de 6 dígitos que llega vía SMS.
- Confirme por llamada telefónica directa la identidad de cualquier familiar o conocido que le solicite dinero de manera urgente.

6. RIESGOS EN REDES WI-FI LOCALES Y DISPOSITIVOS DEL HOGAR (IoT)

Definición:

Una red Wi-Fi doméstica mal configurada o con contraseñas débiles permite que terceros no autorizados se conecten a su red, intercepten el tráfico de datos, consuman su ancho de banda o accedan a dispositivos conectados (*Smart TVs*, cámaras de seguridad, computadores, impresoras).

Medidas de prevención:

- **Contraseña del Wi-Fi:** Cambie la clave predeterminada de su red Wi-Fi por una contraseña segura (combinación de letras mayúsculas, minúsculas, números y símbolos).
- **Seguridad en el Router:** No comparta la clave de su red con personas ajenas a su hogar u organización.
- **Dispositivos IoT:** Si instala cámaras de seguridad o dispositivos inteligentes, cambie siempre las contraseñas que vienen por defecto de fábrica.

CANALES DE ATENCIÓN Y DENUNCIA

En caso de identificar incidentes de seguridad relacionados con su servicio de internet o requerir asesoría técnica sobre la configuración de su red, comuníquese con nuestros canales oficiales:

- **Atención al Cliente PLEXTEL COMUNICACIONES S.A.S.:** *(3132458434)*
- Correo de Soporte: (servicioalcliente@plextelcomunicaciones.com)
- **Sitio Web Oficial:** *(https://plextelcomunicaciones.com/)*

Para denunciar delitos informáticos en Colombia, acuda a los canales oficiales del Estado:

- **Centro Cibernético Policial (CAI Virtual):** caivirtual.policia.gov.co
- **Denuncia Virtual Fiscalía General de la Nación:** adenunciar.policia.gov.co

Las fuentes conceptuales e institucionales principales en las que se basa el contenido son:

Entidades Oficiales de Ciberseguridad en Colombia

- **Policía Nacional de Colombia – Centro Cibernético Policial (CAI Virtual):** Recomendaciones periódicas sobre modalidades de fraude como *phishing*, *smishing*, suplantación de identidad y secuestro de WhatsApp (caivirtual.policia.gov.co).
- **ColCERT (Grupo de Respuesta a Emergencias Ciberseguridad de Colombia):** Guías de prevención sobre *Ransomware*, mitiagción de *Malware* y buenas prácticas de seguridad informática institucional.
- **Fiscalía General de la Nación:** Tipificación de delitos informáticos según la **Ley 1273 de 2009** de Colombia.

2. Organismos y Estándares Internacionales de Seguridad

- **INCIBE (Instituto Nacional de Ciberseguridad):** Estándares y definiciones técnicas accesibles sobre *Phishing*, *Spam*, vulnerabilidad en redes Wi-Fi y dispositivos IoT.
- **Listas Internacionales de Reputación de IP y Anti-Spam:** Estándares operativos de listas de bloqueo de correo masivo como *Spamhaus*, *UCEPROTECT*, *Barracuda* y *DNSStuff*.

3. Marco Regulatorio para Proveedores de Servicios de Internet (ISP)

- **Comisión de Regulación de Comunicaciones (CRC) y Superintendencia de Industria y Comercio (SIC):** Lineamientos e información preventiva que los ISP deben suministrar a sus usuarios respecto a la protección de datos personales (**Ley 1581 de 2012**) y la seguridad en el uso de los servicios de conectividad.