MANUAL DE RIESGOS DE SEGURIDAD DE LA RED - NETSLINK S.A.S.

Netslink S.A.S. - Documento Oficial de Seguridad y Normativa

1. INTRODUCCION Y MARCO CONCEPTUAL

Este manual exhaustivo ha sido diseæado por Netslink S.A.S. para guiar, concientizar y capacitar a nuestros usuarios frente a las amenazas mas recurrentes del ciberespacio. La seguridad digital es un compromiso compartido entre el operador y el usuario final.

2. EL PHISHING Y LA SUPLANTACION DE IDENTIDAD

El phishing es una tecnica de ingenieria social donde atacantes se hacen pasar por Netslink o entidades bancarias para robar informacion personal, financiera o credenciales de acceso.

Como identificarlo: Revise el remitente del correo. Busque errores de ortografia y redaccion. Desconfie de urgencias excesivas o solicitudes de cambio de clave inmediatas.

Buenas practicas: Nunca ingrese a enlaces directos enviados por correo. Escriba la direccion oficial del portal en la barra del navegador.

3. EL AMENAZANTE MUNDO DEL MALWARE Y LOS VIRUS

Los virus, troyanos, ransomware y spyware representan codigo malicioso diseæado para alterar el sistema informatico o secuestrar informacion personal del usuario a cambio de un rescate financiero.

Medidas de proteccion: Mantenga activado el antivirus en su computador y dispositivos moviles. No descargue archivos de paginas no oficiales o torrents dudosos. Aplique las actualizaciones del sistema operativo mensualmente.

4. SPAM Y BUZON DE CORREO NO DESEADO

El correo basura no solo satura el almacenamiento, sino que sirve de vehiculo para propagar enlaces maliciosos.

Mecanismos de control: Utilice los filtros de spam de su proveedor de correo. No responda a correos promocionales no solicitados ni haga clic en 'dar de baja' en remitentes sospechosos.

5. SEGURIDAD EN REDES WI-FI DOMESTICAS

Una red Wi-Fi mal configurada facilita el acceso de terceros a su red local, permitiendoles consumir su ancho de banda o robar datos personales.

Recomendaciones claves: Cambie la contraseæa de administracion de su router ONT entregado por Netslink de forma periodica. Use protocolos de cifrado robustos como WPA2-AES o WPA3. Evite colocar contraseæas obvias como numeros de telefono o fechas de nacimiento.

6. GESTION DE IPS Y REVISION EN LISTAS NEGRAS

En caso de experimentar problemas de navegacion o bloqueo al enviar correos, el usuario puede validar el estado de su direccion IP publica.

Sitios de consulta y tiempos estimados de remocion: Spamhaus (www.spamhaus.org, tiempo estimado 24 horas), Spamcop (www.spamcop.net, tiempo estimado 24 horas), Lashback (www.lashback.com, tiempo estimado 1 hora).