PREVENGA FRAUDES EN SUS COMUNICACIONES

El Estado Colombiano ha concentrado sus esfuerzos en materia de seguridad cibernética, contribuyendo con la alfabetización digital y la implementación de la tecnología 4G como un avance importante para cerrar la brecha digital en el país; sin embargo el auge de dispositivos móviles junto al crecimiento de suscriptores en Internet, han permitido que organizaciones criminales y estafadores saquen provecho del crimen cibernético para lucrarse en medio del anonimato.

Avantel como operador de telecomunicaciones tiene el deber de suministrar a los suscriptores información sobre los riesgos relativos a la seguridad en la red y del servicio contratado que complementan los mecanismos implementados por la compañía para evitar su ocurrencia y a los que puede recurrir el usuario para preservar la seguridad de la red y de las comunicaciones[1].

El **robo de identidad** es uno de los delitos de mayor impacto hoy en día perpetrado por delincuentes que buscan fuera y dentro de internet información personal valiosa. Para mantener un alto nivel de seguridad para prevenir este robo y asegurar las credenciales (usuario y contraseña) que brindan el acceso a servicios en la red desde un PC o dispositivo móvil, recomendamos tener en cuenta:

1. **Use contraseñas no predecibles, extensas (superior a ocho caracteres) y complejas (alfanuméricas y combinadas con caracteres especiales).**
2. **Inicie sesión en su cuenta con frecuencia para asegurarse que no haya actividad inesperada.**
3. **Mantenga antivirus con firmas actualizadas tanto en su computador personal como en su dispositivo móvil.**
4. **Conserve el software (sistema operativo y programas) actualizado con los últimos parches de seguridad emitidos por el fabricante. Por ejemplo mantener la versión más reciente del navegador.**
5. **Compruebe la configuración correcta de su equipo (firewall[2]) para evitar accesos indebidos.**
6. **Configure contraseña fuerte para el enrutador de su red Wi-Fi y otra para acceder a la red inalámbrica; usar la tecnología de encriptación más fuerte.**
7. **Tenga precaución con enlaces recibidos en mensajes de correo electrónico y chat de cuentas desconocidas.**
8. **Este alerta de correos electrónicos que solicitan o inician una actividad pirata para obtener información personal delicada o a través de ventanas emergentes fraudulentas y sitios Web.**
9. **Codifique los documentos importantes o confidenciales con contraseñas robustas.**
10. **Evite proporcionar número de identificación, número de tarjeta o cualquier detalle de cuentas bancarias por teléfono, a menos de tener la certeza que se trata de una comunicación confiable.**
11. **No olvide sobres que contengan pagos de cuentas de tarjetas de crédito, servicios públicos o documentos confidenciales, si es el caso usar la trituradora de papeles para deshacerse de ellos.**
12. **No anote claves, números de tarjetas de crédito, datos financieros o personales en papeles o dejarlos visibles al alcance de terceros.**

---

[1] CRC. Resolución 3066 de 2011, En: "Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones" [PDF]. <http://www.crcom.gov.co/?idcategoria=61450&download=Y> [citado el 15 de julio de 2014]

[2] "Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas" [ON LINE]. <http:// es.wikipedia.org/wiki/Cortafuegos_(informática)>

Existen **correos electrónicos y sitios web falsos** (phishing[3]) diseñados para engañar y que resultan difícil de distinguir de los reales: La práctica más recomendable es evitar dar clic en vínculos embebidos en contenido no confiable, abrir el navegador, escribir la URL del sitio e ingresar con la cuenta respectiva. Cuatro indicadores de un correo electrónico fraudulento son los siguientes:

1. **El remitente del correo electrónico pudo haber sido modificado con facilidad y el nombre no brinda la validez de una comunicación emitida de una cuenta autentica.**
2. **El saludo genérico en un correo electrónico es una muestra de falta de confianza, generalmente los saludos son personalizados citando nombre y apellidos.**
3. **La falsa sensación de urgencia en el contenido del mensaje para conseguir información confidencial.**
4. **Vínculos falsos y archivos adjuntos son peligrosos, podrían descargar spyware o virus para robar la información que se digita a través del teclado.**

El uso de código malicioso para lograr **acceso abusivo a los sistemas** es otra de las tendencias que afectan el entorno de las telecomunicaciones, principalmente las **centrales telefónicas privadas (PBX)** donde se busca control o acceso a la configuración del servidor para comprometerlo con el fin de vender o realizar llamadas sin consentimiento del propietario. Algunas de las recomendaciones para fortalecer el servidor y detectar rápidamente ataques son las siguientes:

1. **Desactive la configuración por defecto en el servidor (p.e.: puerto SSH 22/TCP, contraseñas predeterminadas)**
2. **Utilice la autenticación de clave publica/privada en lugar de uso de contraseña.**
3. **Cree una cuenta de usuario y desactivar el inicio de sesión como "root".**
4. **Realice restricción geográfica de direcciones IP (p.e.: China, Ucrania, Rusia, etc.) para evitar su registro y acceso al servidor.**
5. **Evalue separar la red VoIP de la red de datos.**
6. **No exponga el servidor VoIP o PBX a internet.**
7. **Implemente túneles SSH para acceder a la interfaz grafica de administración.**
8. **Utilice contraseñas seguras para las extensiones remotas.**
9. **Utilice Sistemas de Detección de Intrusos como Fail2Ban o Snort.**
10. **Mantenga actualizada las versiones y parches**
11. **Haga énfasis en educación, entrenamiento y sensibilización a los trabajadores sobre ataques VoIP, pueden ser la diferencia para evitar intrusiones o fuga de información a la red corporativa.**

Para mayor información realice una revisión completa de sus servidores de comunicación VoIP para identificar vulnerabilidades desconocidas que puedan ser explotadas por un atacante informático.

[3] "Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria)" [ON LINE]. <http://es.wikipedia.org/wiki/Phishing>