EQUARED

Para Equared S.A.S su seguridad es importante.
A continuación, se expondrán algunas recomendaciones para el uso seguro del servicio de internet y la transmisión de datos.

Privacidad y contraseñas
La elección correcta de usuarios y contraseñas es de suma importancia para la seguridad informática, por ende, es fundamental que el cliente acate y aplique los correctivos para evitar ser víctimas de ataques y/o fraudes electrónicos.

Recomendaciones:

- ✓ El usuario y contraseña es personal, ninguna persona que no sea el titular del servicio, debería tener acceso a estos.
- ✓ No utilizar contraseñas obvias o que provengan de información personal, por ejemplo: nombre del cliente, nombre de mascotas, nombre de familiares, artistas preferidos, cedula de identidad, teléfonos de contacto, fechas de nacimiento, etc.
- ✓ Cambiar la contraseña de manera periódica, por lo menos cada 6 meses.
- ✓ Tener una longitud de 8 o más caracteres, mientras más larga se la contraseña, será más difícil de vulnerar.
- ✓ En los dispositivos que soporten diferentes caracteres, se deberían mezclar caracteres alfabéticos (A..Z, a...z), numéricos (0...9) y especiales (!"$%&@)ademas de alternar entre mayúsculas y minúsculas.

Pishing (Suplantación de identidad)
Pishing es la practica fraudulenta de suplantación de sitios web realizada por estafadores que buscan atraer con engaños a los consumidores y sustraer su información personal o financiera, enviando correos electrónicos o utilizando mensajes de aparición automática en sitios web (pop-up ads).

Recomendaciones:

- ✓ No responder mensajes mediante correo electrónico o de aparición automática (pop-up ads), en donde se pida información personal o financiera, ni hacer clic en ninguno de este tipo de anuncios.
- ✓ No utilizar la función copiar y pegar para colocar enlaces en el navegador web, debido a que los ‘’pishers’’ (pescadores de información) pueden conseguir que los vínculos aparenten llevarlos al sitio web deseado, pero realmente lo conectan a uno diferente.

- ✓ Las entidades bancarias nunca le pedirán su número secreto por correo electrónico. Los números secretos deben ser utilizados solo en las páginas oficiales de la entidad bancaria.
- ✓ Verificar que la dirección del sitio web inicie con la determinación del protocolo "https://" en lugar de "http://" que es el que se encuentra normalmente en las páginas web.
- ✓ No enviar información personal o financiera por correo electrónico.
- ✓ Revisar los estados de cuenta tan pronto como se reciban, para constatar que no se hayan realizado cargos no autorizados.
- ✓ Tener precaución al abrir archivos electrónicos adjuntados o al descargar archivos de correos electrónicos recibidos.
- ✓ Reenviar los mensajes de "phishing" a la compañía, entidad bancaria u organización cuyo nombre fue falsamente invocado como remitente del mensaje.
- ✓ No perder atención mientras se encuentren abiertos sitios web de servicios financieros.
- ✓ Cuando se deje de utilizar aplicaciones o páginas web de entidades bancarias siempre utilizar la opción "SALIR".
- ✓ En caso de extraviar tarjetas de acceso a servicios financieros, es necesario comunicarse con la entidad bancaria y realizar el bloqueo de esta.

Si usted fue afectado por este tipo de ataque, puede acceder a los servicios de la Fiscalía General de la Nación o Defensoría del Pueblo.

Protección infantil

Actualmente el uso de las tecnologías de información por parte de los niños se realiza desde tempranas edades, el internet es una herramienta importante para el aprendizaje de los niños, pero así mismo se debe tener en cuenta que la libertad de navegación en este medio es notoriamente peligrosa.

Es deber de los padres el control de uso de las tecnológicos y el acceso a servicios de internet.

Recomendaciones:

- ✓ Supervisar a niños o adolescentes al momento de usar esta herramienta.
- ✓ Contar con aplicaciones que faciliten el control de contenido y así filtrar la información que sea adecuada para el menor.