

Sepa como protegerse de e-mails fraudulentos

Manejo de Claves Secretas o Passwords .

Las claves de seguridad son las llaves que le permiten acceder y operar con sus cuentas.

Para minimizar el riesgo de que alguien acceda a las mismas, evite usar las mismas claves para distintos servicios.

Algunos consejos sobre el manejo de claves:

- Es recomendable no utilizar claves fácilmente adivinables, por ejemplo: fechas de nacimiento, teléfonos o números de cliente o cuenta.
- Cambie periódicamente sus claves secretas.
- Nunca facilite sus claves o contraseñas a nadie, especialmente si se las requieren a través de un email.
- Memorice sus claves y nunca las anote. Si no tiene más remedio, hágalo de forma que no se note que son sus claves.
- Al ingresar su clave en cajeros automáticos o comercios, verifique que únicamente usted puede ver la información que está ingresando.

Cuando navegue en Internet recuerde tener en cuenta:

- Navegar en sitios seguros. Puede verificar si el sitio está certificado buscando el sello de empresas como Verisign y en la barra inferior vea un candado. Además es prudente verificar en la barra del explorador que la dirección del sitio comience por https (con la s de secure, es decir seguro).
- Abrir solamente los correos electrónicos de personas conocidas.
- Tener cuidado al abrir correos electrónicos con archivos adjuntos.
- Mantener actualizado su antivirus. Descargue las últimas versiones de los anti-virus tan pronto éstas estén disponibles.
- Mantener actualizado el navegador de Internet (Internet Explorer, Firefox, Opera, etc), ya que muchas veces explotan vulnerabilidades de los mismos.

Prevención y fraudes usando Internet

Los correos electrónicos fraudulentos (o Phishing) son enviados como spam (correo no solicitado). Phishing es la duplicación de una página web que busca hacer creer que el lector o visitante se encuentra en la página original en lugar de la copiada.

Es frecuente que se utilice para duplicar páginas web de bancos de prestigio y se envíen indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

Los ataques de Phishing usan ingeniería social y subterfugios técnicos para robar los datos personales y claves de acceso financieras. Usan emails falsos para guiar a los clientes a sitios falsos diseñados para engañar a los visitantes para que divulguen información financieras, como números de tarjetas de crédito, nombres de usuarios, claves o contraseñas y hasta documentos de identidad. Suplantando nombres de bancos, proveedores de ecommerce, y compañías de tarjetas de crédito, los delincuentes frecuentemente convencen a las personas de responder.

Como el Phishing busca capturar información confidencial del cliente, los emails son preparados muy detalladamente, de forma que parezcan mails realmente enviados por la entidad bancaria. Es por eso que se copian los logos, signos, colores y fotografías que habitualmente el banco usa en su identidad.

Crédit Uruguay Banco nunca enviará correos con el objeto de que verifique el nombre de usuario, claves de acceso, números de tarjeta de crédito o cualquier otra información confidencial.

Este tipo de correos siempre son denunciados e investigados para determinar su procedencia y aplicación de las leyes correspondientes.

Como prevenir el Phishing

- Recuerde que Crédito Uruguay Banco nunca enviará correos con el objeto de que verifique el nombre de usuario, claves de acceso, números de tarjeta de crédito o cualquier otra información confidencial.
- Antes de ingresar cualquier información confidencial, busque el candado en la barra inferior del navegador para asegurarse que el sitio está certificado como seguro.
- Evite hacer clicks en links o vínculos contenidos en correos electrónicos, estos links pueden llevarlo a un sitio web falso, con aspecto similar a uno verdadero.
- Opere siempre en computadores conocidos, evitando la utilización en cybercafés o computadores de uso público.
- Esté alerta de correos electrónicos que le soliciten revelar información confidencial, aunque conozca su remitente.
- No conteste ningún correo electrónico que solicite su información personal incluyendo alguna contraseña, número de cédula u otra información confidencial. Haga compras online solamente en sitios que usted confía. No envíe información personal o financiera a través de correos electrónicos.
- **Para acceder a e-banca, siempre digite en la barra del explorador de Windows la dirección del banco (<https://www.credituruguay.com.uy>).**

¿Qué debe hacer frente a un email fraudulento?

Si usted recibe un email o correo electrónico fraudulento:

1. Salga inmediatamente de la página que usted cree que no son lo que pretenden ser.

- 2.** No siga ninguna de las instrucciones que aparecen en el email, pop-up o página web.
- 3.** Informe a la brevedad al Banco, llamando al (02) 1929 o al (005982) 915 0225, si está en el exterior. También puede escribir a servicioalcliente@credituruguay.com.uy o concurrir a cualquiera de nuestras sucursales.
- 4.** Si ya ingresó información confidencial en un sitio que considera inseguro, por favor comuníquese de inmediato con el Banco, con el objeto que se tomen las medidas preventivas para evitar un posible fraude.