Online Security Tips

While GBC is committed to ensure the highest standard of security on our systems, you as the end-user also play an important role to ensure that you are adequately protected when you use the Internet. The following security best practices are recommended:

- Install anti-virus, anti-spyware and other internet security software on your PC. Use it regularly and keep it up-to-date.
- Take advantage of your PC's security features. Make sure your browser uses the strongest encryption available and be aware of the encryption levels of the sites and applications you use.
- Regularly update your PC's operating system and Web browser software with the vendor's software patches and updates to protect your PC against known vulnerabilities.
- Do what you can to prevent unauthorized people from using your PC.
- Change your passwords often. Be sure to choose passwords that are hard for others to guess.
- Do not download or open any attachments sent to you by unsolicited email. Once opened, these programs may contain malicious programs that can compromise your PC's security.
- Be on the alert for phishing scams. Access Web sites by typing the Web addresses directly into your Web browser or by using Web addresses you have bookmarked, instead of via embedded links in unsolicited emails.

If you feel you may have received a fraudulent email appearing to come from Green Bull Capital, please contact our client service team, or email us at (info@greenbullcapital.com).

Consejos de seguridad en línea

Mientras GBC se compromete a garantizar el más alto nivel de seguridad en nuestros sistemas, usted, como usuario final también juega un papel importante para asegurar que esté adecuadamente protegido cuando utiliza Internet. Se recomiendan las mejores prácticas de seguridad siguientes:

- Instale anti-virus, anti-spyware y otro software de seguridad de Internet en su PC. Utilícelo regularmente y manténgalo al día.
- Aproveche las características de seguridad de su PC. Asegúrese de que su navegador utiliza el cifrado más potente disponible y sea consciente de los niveles de cifrado de los sitios y aplicaciones que utiliza.
- Actualice regularmente el software del sistema operativo y el navegador Web de su PC con los parches y actualizaciones de software del proveedor para proteger su PC contra vulnerabilidades conocidas.
- Haga lo que pueda para evitar que personas no autorizadas utilicen su PC.
- Cambie sus contraseñas con frecuencia. Asegúrese de elegir contraseñas difíciles de adivinar.
- No descargar o abrir los archivos adjuntos enviados por correo electrónico no solicitado. Una vez abierto, estos programas pueden contener programas maliciosos que pueden comprometer la seguridad de tu PC.
- Esté alerta de estafas de phishing. Acceda a los sitios web escribiendo las direcciones Web directamente en el navegador Web o mediante el uso de las direcciones Web que ha marcado, en lugar de a través de los enlaces incorporados en correos electrónicos no solicitados.

Si usted siente que puede haber recibido un correo electrónico fraudulento que aparece venir de Green Bull Capital, por favor póngase en contacto con nuestro servicio de atención al cliente, o envíenos un e-mail a info@greenbullcapital.com.