CONSEJOS DE SEGURIDAD SOBRE PHISHING

Es importante protegerse usted y a otros contra todos los ataques de phishing y no causar daño a otros de forma accidental. Estas son algunas de las mejores prácticas que lo ayudarán a usted lograr esto:

QUÉ DEBERÍA HACER

- Abra archivos adjuntos solo si son de una fuente conocida y si usted está esperándolos.
  - Si está esperando uno, llame a la persona involucrada y verifique el correo antes de abrirlo.
- Si un correo electrónico lo amenaza con consecuencias graves, verifique a través de un canal diferente.
- Antes de hacer clic en cualquier enlace, mueva el ratón sobre el enlace y lea el URL completo para verificar que el enlace es auténtico.
- Escriba los enlaces directamente en el navegador, en lugar de hacer clic en estos.
- Verifique el remitente de correos electrónicos sospechosos, incluso si el correo electrónico es de una persona conocida.
  - El dominio de estos correos electrónicos no sería uno auténtico.

QUÉ DEBERÍA EVITAR

- Evite abrir correos electrónicos desconocidos con archivos adjuntos, enlaces para hacer clic, correos de premios, correos de pánico y correos de amenazas.
  - Mientras más atractivo sea el premio = más es la posibilidad de un ataque.
  - Ignore estos correos, a menos que usted esté esperando un premio.
- Evite sitios web que parezcan sospechosos.
- No use, distribuya ni cree virus, gusanos u otro software malicioso de manera intencional.
- No interrumpa ni cambie los ajustes del escaneo de autovirus programado en su computadora de escritorio/portátil.

- Tenga cuidado con correos electrónicos desconocidos que indican urgencia o acciones inmediatas.
  - Verifique estos correos electrónicos con equipos de seguridad /IT.
- Busque problemas tales como:
  - Mal formateo de correo electrónico
  - Eslogan y logotipos borrosos
  - Mala ortografía y gramática
  - Saludos y mensajes genéricos

- Absténgase de compartir información personal o sensible relacionada con ABI en correos electrónicos o formularios web.
- Evite abrir correos electrónicos marcados como correo basura.
  - ABI tiene herramientas para filtrar y marcar comunicación como correo basura.

Recuerde siempre reportar oportunamente lo siguiente:

- Correos electrónicos sospechosos
- Virus/Incidentes con software

Reporte siempre esta actividad de phishing a:

soc-support@ab-inbev.com