BPAS

Política de Ciberseguridad

Una adición al estado de política relativo a las transacciones de cuentas en BPAS

Hoy en día, datos sobre los consumidores estadounidenses están en todas partes. Proteger la seguridad de sus cuentas de retiro es una de las prioridades principales de BPAS; sin embargo, no podemos hacerlo solos. Proteger las cuentas de los participantes es una responsabilidad compartida entre los patronos, los proveedores de servicios, y los participantes. Esta política de ciberseguridad describe los pasos que debe tomar como participante para mejorar sus posibilidades de recuperación si se produce alguna actividad fraudulenta o robo de identidad dentro de su cuenta y también resalta el compromiso de BPAS sobre este asunto importante.

Como parte rutinaria de nuestros procedimientos de seguridad, BPAS realiza auditorías periódicas de nuestra infraestructura de Tecnología Informática. Los firewalls, el software antivirus y las correcciones de seguridad se encuentran entre las medidas que utilizamos para proteger nuestros sistemas. Nuestros sitios web se basan en el cifrado estándar de la industria para proteger la transmisión y el acceso a los datos. Nuestro personal monitorea de cerca las alertas de seguridad y aplica actualizaciones según sea necesario.

Le recomendamos que utilice un navegador compatible con encriptación, habilitado para JavaScript, y que acepte cookies. Estas medidas nos permiten dar seguimiento del uso del sitio web y mejorar nuestro servicio.

Es mejor que utilice la última versión de uno de estos navegadores para acceder a su cuenta de BPAS: Internet Explorer, Firefox, Google Chrome o Safari.

BPAS continuará identificando nuevas herramientas e implementando funciones en nuestros sistemas en línea para ayudar a garantizar la protección de sus datos y activos.

Aunque estas herramientas y funciones le ayudan, usted es el elemento más crítico para proteger su cuenta.

Consejos para la prevención del fraude

- Si le hacen una oferta que parezca demasiado buena para ser verdad, probablemente lo es.
- Un atacante intentará afectar tus emociones, para que sientas urgencia o miedo, con el fin de que actúes rápidamente.
- Limite la información que usted pone en sus perfiles de las redes sociales. Un atacante puede utilizar estos sitios para recopilar información valiosa y utilizarla para cometer fraude contra usted o sus familiares o amigos. Además, ten cuidado con los juegos o pruebas en tus redes sociales. Muchas de estas pruebas son creadas por estafadores que buscan recopilar información personal sobre usted, como nombres de miembros de la familia, fechas importantes, colores favoritos, etc. Esta información hace que sea más fácil para ellos hacerse pasar por usted y responder preguntas de seguridad.
- Cuestione los correos electrónicos no solicitados que contienen archivos adjuntos, especialmente si requieren que habilite las macros, ya que son potencialmente maliciosos.
- Tenga presente que una cuenta de correo electrónico de un amigo o pariente podría verse comprometida. Los atacantes pueden falsificar la dirección de correo electrónico de un remitente para que parezca ser de cualquier persona que elijan. Si recibe un correo electrónico sospechoso, comuníquese con esa persona de quien parece ser el correo para confirmar si lo enviaron.
- Algunos de los lugares más comunes donde se producen ataques de ingeniería social son por correo electrónico, mensajes de texto, o incluso por teléfono.
- Las estafas a menudo comienzan con llamadas telefónicas de un atacante que afirma que son soporte técnico de una compañía conocida. Intentarán convencerlo de que su computadora está infectada con virus. Debe colgar el teléfono de inmediato.
- Cuando inicie sesión en su cuenta de BPAS o transmita información confidencial, acceda la página directamente utilizando la dirección en la URL. No haga clic en los enlaces de un correo electrónico o motor de búsqueda. Asegúrese también de que la dirección en la URL muestra que es un sitio seguro (https, no http).
- Use secure protocols and the BPAS secure messaging center when transmitting confidential information; email should be a last resort, because it can become compromised.
- Mantenga sus navegadores de Internet actualizados. Asegúrese de que el buzón de correo de su casa esté seguro o utilice una PO Box.
- Instale protección antivirus y contra malware en su computadora(s) y active las actualizaciones automáticas.
- No abras correos electrónicos o archivos adjuntos de remitentes que no conozcas o que parezcan sospechosos.

BPAS

Pasos de Seguridad Recomendados y Necesarios

A continuación, se muestra una lista de los pasos **recomendados** y **necesarios** que debe tomar para proteger su cuenta y aumentar sus posibilidades de recuperación en caso de fraude externo. Si se sospecha que ha ocurrido fraude dentro de la cuenta de un participante, BPAS investigará la situación con las instituciones financieras apropiadas y la policía para determinar los pasos de seguimiento y la responsabilidad de todas las partes. El tiempo que tome este proceso para resolver cualquier disputa será impulsada por instituciones externas y la aplicación de la ley. Su capacidad para conseguir recuperaciones dependerá de las acciones que tome para proteger su cuenta como se refleja a continuación.

Pasos	Recomendado	Necesario
Cree un ID de usuario que sea único para usted y que no sea fácil de adivinar. No use su número de seguro social o dirección de correo electrónico como su ID de usuario.	✔	✔
Usa una contraseña segura en tu cuenta: • Siga los parámetros requeridos que combinan letras, números y símbolos • Evite patrones de teclado predecibles • No utilice la misma contraseña para varios sitios y cuentas • No utilice su ID de usuario como contraseña • Nunca compartas su contraseña • Cambie la contraseña cada 90 días, o inmediatamente si crees que ha sido comprometida.	✔	✔
No almacene su ID de usuario y contraseña en su teléfono, excepto en una aplicación segura para mantener la contraseña, y no seleccione "Recordar contraseña" en su navegador.	✔	
Inicie sesión y revise su cuenta de BPAS al menos una vez al mes.	✔	
Actualice su cuenta en u.bpas.com para incluir una dirección de correo electrónico personal actual que monitoreas y accedas regularmente. Es preferible que el email sea uno que será **visible en su teléfono móvil inmediatamente cuando reciba un correo electrónico**. BPAS le enviará alertas por correo electrónico cuando se inicien o intenten cambios en la cuenta.	✔	✔
Monitorea los correos electrónicos que recibes de BPAS, revisa la actividad de la cuenta y notifícanos inmediatamente (en el plazo de 1 día laboral) de cualquier actividad cuestionable.	✔	✔
No inicie sesión en su cuenta de BPAS desde una computadora pública ni use WIFI público.	✔	✔
Cumplir de buena fe si le pedimos su cooperación en una investigación (incluyendo que una compañía profesional de seguridad informática revise su computadora, investigación policial, etc.).	✔	
Chequear su buzón frecuentemente teniendo pendiente cualquier correspondencia de BPAS. Abra y revise rápidamente todos los estados de cuenta y confirmaciones enviadas.	✔	✔
Asegúrese de que su dirección postal esté actualizada en BPAS en todo momento..	✔	
No utilice un servicio de agregación de cuentas que requiera que envíe su ID de usuario o contraseña a una empresa externa.	✔	✔
No haga clic en enlaces ni abra archivos adjuntos en correos electrónicos de remitentes desconocidos para usted.	✔	
Mantenga el spyware actualizado en su computadora de casa y/o portátil.	✔	
BPAS nunca le pedirá que proporcione información personal o de su cuenta por correo electrónico. Notifique BPAS dentro de las 24 horas si sospecha o nota actividad sospechosa en su cuenta o por correo electrónico.	✔	

¿Preguntas? Hablemos.

Proteger la seguridad de sus cuentas es una tarea compartida, y estamos aquí para ayudarlo.
Por favor, póngase en contacto con cualquier pregunta o inquietud.

emailfraud@bpas.com | u.bpas.com | 1.866.401.5272