BENEFIT MATTERS

April
Abril
2022

8 ways to protect your personal information

You can reduce the risk of theft, fraud and loss to your online data by following these basic rules:

1. **Register, set up and routinely monitor your online financial accounts.**

   Creating an online account to access and monitor your banking, savings and retirement accounts allows you to both protect and manage your account at the same time. Regularly checking your retirement and financial accounts reduces the risk of fraudulent account access. Continued inside

8 modos de proteger su información personal

Usted puede reducir el riesgo de robo, fraude y pérdida de sus datos online siguiendo estas normas básicas:

1. **Registre, configure y supervise con frecuencia sus cuentas financieras online.**

   Crear una cuenta online para acceder y supervisar sus cuentas bancarias, de ahorros y de jubilación le permite proteger su cuenta y gestionarla al mismo tiempo. La comprobación regular de sus cuentas de jubilación y financieras reduce el riesgo de acceso fraudulento a las cuentas. Continúa adentro

NEWS YOU CAN USE

For more information

See inside to learn more about how you can protect your personal information.

NOTICIAS ÚTILES

Para obtener más información

Vea adentro para aprender más sobre cómo proteger su información personal.

FOR MORE ABOUT YOUR BENEFITS CALL MEMBER SERVICES at **800-551-3225** or visit **www.32bjfunds.org** or email **benefitmatters@32bjfunds.com**

PARA SABER MÁS SOBRE SUS BENEFICIOS, LLAME A SERVICIOS A AFILIADOS, al **800-551-3225,** visite **www.32bjfunds.org** o escriba por email a **benefitmatters@32bjfunds.com**

8 WAYS TO PROTECT YOUR PERSONAL INFORMATION

Continued from the front

2. **Use strong and unique passwords.**
   - Don't use dictionary words.
   - Use letters (both upper and lower case), numbers, and special characters.
   - Don't use letters and numbers in sequence (nothing like "abc" or "567").
   - Use 14 or more characters.
   - Don't write passwords down.
   - Consider using a secure password manager to help create and track passwords.
   - Change passwords every 120 days, or if there's a security breach.
   - Don't share, reuse or repeat passwords.
3. **Use multi-factor authentication.**

   Multi-factor authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).
4. **Keep personal contact information current.**

   Update your contact information when it changes, so you can be reached if there's a problem. Select multiple communication options.
5. **Close or delete unused accounts.**

   The smaller your online presence, the more secure your information. Close unused accounts to minimize your vulnerability. Sign up for account activity notifications.
6. **Be wary of free Wi-Fi.**

   Free Wi-Fi networks – such as the public Wi-Fi available at airports, hotels or coffee shops – pose security risks that may give criminals access to your personal information. A better option is to use your cellphone or home network.

7. **Beware of phishing attacks.**

   Phishing attacks aim to trick you into sharing your passwords, account numbers and sensitive information to gain access to your accounts. A phishing message may look like it comes from a trusted organization to lure you to click on a dangerous link or pass along confidential information. (See box below.)
8. **Use antivirus software and keep apps and software current.**

   Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

Common warning signs of phishing attacks include:

- A text message or email that you didn't expect or that comes from a person or service you don't know or use.
- Spelling errors or poor grammar.
- Mismatched links (a seemingly legitimate link sends you to an unexpected address). Often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination.
- Shortened or odd links or addresses.
- An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information or answers to security questions).
- Offers or messages that seem too good to be true, express great urgency or are aggressive and scary.
- Strange or mismatched sender addresses.
- Anything else that makes you feel uneasy.

8 MODOS DE PROTEGER SU INFORMACIÓN PERSONAL

Viene de la portada

2. **Elija contraseñas fuertes y únicas.**
   - No utilice palabras del diccionario.
   - Incluya letras (tanto mayúsculas como minúsculas), números y caracteres especiales.
   - No use letras y números en secuencia (evite series como "abc" o "567").
   - Use 14 caracteres o más.
   - No escriba las contraseñas en papel.
   - Considere usar un gestor de contraseñas que le ayude a crear y mantener un registro de las contraseñas.
   - Cambie de contraseña cada 120 días, o cada vez que haya una brecha de seguridad.
   - No comparta, reutilice ni repita contraseñas.
3. **Use autenticación multifactorial.**
   La autenticación multifactorial (también llamada autenticación con dos factores) requiere emplear una segunda credencial para verificar su identidad (por ejemplo, introducir un código enviado en tiempo real por mensaje de texto o correo electrónico).
4. **Mantenga actualizada la información de contacto personal.**
   Actualice su información de contacto cada vez que la cambie, para que puedan comunicarse con usted si surge un problema. Seleccione varias opciones de comunicación.
5. **Cierre o borre las cuentas que no utilice.**
   A menor presencia online, más segura estará su información. Cierre las cuentas que no use para minimizar su vulnerabilidad. Active recibir notificaciones sobre la actividad de su cuenta.

6. **Tenga cuidado con el Wi-Fi gratuito.**
   Las redes de Wi-Fi gratis – como la Wi-Fi pública disponible en aeropuertos, hoteles o cafeterías – crean riesgos de seguridad que pueden permitir el acceso de los delincuentes a su información personal. Una opción mejor es usar su celular o la red de Internet de su casa.
7. **Tenga cuidado con los ataques de phishing.**
   Los ataques de phishing buscan engañarle para que comparta sus contraseñas, números de cuenta e información sensible y lograr acceder a sus cuentas. Un mensaje de phishing puede tener la apariencia de que procede de una organización confiable para incitarle a pulsar en un enlace peligroso o introducir información confidencial. (Mire el recuadro más abajo.)
8. **Utilice antivirus y mantenga las apps y el software al día.**
   Asegúrese de tener instalado y actualizado un programa antivirus que proteja sus computadoras y dispositivos móviles frente a virus y malware. Mantenga todo su software con los últimos parches y mejoras. Muchos proveedores ofrecen actualizaciones automáticas.

Las señales de advertencia más comunes de los ataques de phishing son:

- Un mensaje de texto o de correo electrónico que no esperaba o que viene de una persona o servicio que usted no conoce o no utiliza.
- Errores de ortografía o de gramática.
- Enlaces que no cuadran (un enlace aparentemente legítimo le envía a una dirección inesperada). Con frecuencia, aunque no siempre, puede detectarlo pasando el ratón por encima del enlace sin pulsar en él para que el navegador le muestre el destino real.
- Enlaces o direcciones acortados o extraños.
- Un mensaje de correo electrónico que le pida su número de cuenta o información personal (los proveedores legítimos nunca envían correos electrónicos o mensajes de texto pidiendo la contraseña, el número de cuenta, la información personal o respuestas a preguntas de seguridad).
- Ofertas o mensajes que parecen demasiado buenos para ser verdad, que expresan una gran urgencia o que son agresivos y atemorizantes.
- Direcciones de envío extrañas o desparejas.
- Cualquier otro detalle que le provoque una sensación de incomodidad.

ONLINE SECURITY TIPS

Cybersecurity or online security is important because it protects your online information from theft and damage.

Cybersecurity protection safeguards the following online information:

- Personal information (your name, Social Security number, your driver's license, bank account number(s), passport, email address)
- Protected health information (medical history, diagnoses, treatments, medications)
- Retirement benefit information
- Savings information

FOR MORE INFORMATION, SEE INSIDE.

CONSEJOS DE SEGURIDAD ONLINE

La ciberseguridad, o seguridad online, es importante porque protege su información de Internet frente a robos y daños.

La protección de ciberseguridad salvaguarda la siguiente información online:

- Información personal (su nombre, número de Seguro Social, su licencia de manejar, los números de sus cuentas bancarias, su pasaporte, su dirección de correo electrónico)
- Información de salud protegida (historia clínica, diagnósticos, tratamientos, medicaciones)
- Información sobre los beneficios de la jubilación
- Información sobre los ahorros

PARA MÁS INFORMACIÓN, VEA ADENTRO.

Building Service 32BJ Benefit Funds
25 West 18th Street
New York, NY 10011

NON PROFIT
U.S. POSTAGE
PAID
MVPRINT

IMPORTANT / IMPORTANTE

HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS

The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:

- www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
- www.cisa.gov/reporting-cyber-incidents

CÓMO REPORTAR UN ROBO DE IDENTIDAD O INCIDENTES DE CIBERSEGURIDAD

El FBI y el Department of Homeland Security (Departamento de Seguridad Nacional) tienen sitios Web muy útiles para reportar los incidentes de ciberseguridad:

- www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
- www.cisa.gov/reporting-cyber-incidents