

Cyber Security and Your Carpenter Benefits



Keeping your financial and benefits information secure is important. There are some simple steps you can take to help keep your private information safe and secure.

What you Can Do

Password Security - Keep your passwords safe - Don't share your passwords with anyone, and don't use the same password in multiple places.

Password Strength - Make sure your passwords are strong

- Avoid using simple words or strings of numbers ("1234")
- Abbreviate words, misspell on purpose, and add capital letters
- Combine letters and numbers and include special characters like !, # or &
- Make sure your password is long and complex

For example, use "1drfulMrning!" instead of "wonderfulmorning"

Watch out for "Phishing" and Scammers



Phishing (pronounced: fishing) is an attack where cybercriminals send a fake message that attempts to steal your money or identity by getting you to click on malicious links or reveal personal information on websites that pretend to be legitimate.

- Do not respond to or click links on emails or texts unless you're sure of the source
- Double-check web addresses and links before you click
- Don't trust anyone who contacts you and requests personal information

Keep Devices Current and Secure

- Don't share devices you use to access your benefits information, and keep your passwords to yourself
- Make sure the software on your devices is up to date
- Lock your device with a passcode or biometric recognition (fingerprint or eye scan)
- If your phone is lost or stolen, remotely erase the data; contact your service provider for instructions
- Do not use public wifi to access your private information

What We do to Protect You - Your accounts, data and privacy are our highest priority. Among other things:

- The Fund Office follows HIPAA protocols to ensure your private health information is secure. HIPAA (Health Insurance Portability and Accountability Act of 1996) is a law that defines how your health information is protected, strictly limiting its sharing and use.
- Your financial information is just as important. The Fund Office protects your data with state of the art security, our staff is trained to avoid malicious attacks, and our Benefits Portal uses two-factor authentication to make sure only you can see your accounts and benefits information.
- We use advanced firewalls to help prevent website attacks, and use credential stuffing protection to prevent automated account login attempts.



Working together, we can keep hackers out, and your data and accounts safe and secure.



La seguridad cibernética y sus beneficios como carpintero

Es importante que mantenga segura su información financiera y la de sus beneficios. Usted puede tomar algunos pasos sencillos para ayudar a mantener su información privada segura y protegida.

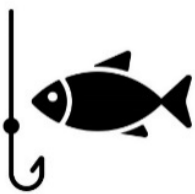
Lo que puede hacer

Seguridad de sus contraseñas - Conserve seguras sus contraseñas. No las comparta con nadie, y no use la misma contraseña en varios lugares.

Resistencia de las contraseñas - Asegúrese de que sus contraseñas sean resistentes

- Evite usar palabras sencillas o secuencias de números (“1234”)
- Abrevie palabras, escribalas mal intencionalmente y añada letras mayúsculas
- Combine letras y números e incluya caracteres especiales como !, # o &
- Asegúrese de que su contraseña sea larga y compleja

Por ejemplo, use “1mvlsmñ!” en lugar de “maravillosamana”



Manténgase alerta a la suplantación de identidad “Phishing” y a los estafadores

La suplantación de identidad (*phishing*) es un ataque en el que los cibercriminales envían mensajes electrónicos falsos para robarle su dinero o su identidad haciendo que usted haga clic en enlaces fraudulentos o que revele información personal en sitios web que pretenden ser legítimos.

- No responda ni haga clic en enlaces que reciba en mensajes electrónicos o de texto, a menos que esté seguro de la fuente
- Verifique dos veces las direcciones y los enlaces antes de hacer clic
- No confíe en nadie que se comunique con usted y le pida información personal

Mantenga sus dispositivos actualizados y seguros

- No comparta los dispositivos que usa para acceder a la información sobre sus beneficios, y conserve privadas sus contraseñas
- Asegúrese de que el software de sus dispositivos está actualizado
- Bloquee su dispositivo con una contraseña o con reconocimiento biométrico (huella digital o escaneo del ojo)
- Si pierde o le roban su teléfono, borre remotamente los datos y llame a su proveedor de servicio para que le den instrucciones
- No use el wifi público para acceder su información privada

Lo que hacemos para protegerlo - Sus cuentas, datos y privacidad son nuestra principal prioridad. Entre otras cosas:

- La Oficina del Fondo sigue los protocolos de la Ley de Responsabilidad y Transferencia del Seguro Médico de 1996 (The Health Insurance Portability and Accountability Act of 1996, HIPAA) para asegurarse de que su información médica privada esté segura. La HIPAA es una ley que define cómo se protege su información médica y limita estrictamente su compartición y uso.
- Su información financiera es igualmente importante. La Oficina del Fondo protege sus datos con medidas de seguridad de vanguardia, nuestro personal está capacitado para evitar ataques malintencionados, y nuestro portal de beneficios usa un método de autenticación de dos factores para asegurarse de que solo usted pueda ver la información sus cuentas y de sus beneficios.
- Usamos paredes cortafuegos para ayudar a prevenir ataques a nuestro sitio web, y usamos protección contra ciberataques automatizados (*credential stuffing*) para prevenir intentos automatizados de iniciar sesiones en las cuentas.



Al trabajar conjuntamente, podemos mantener a los piratas informáticos alejados y sus datos y cuentas seguros y protegidos.