

Is e-mail I send to you secure? Absolutely not! E-mail is sent as clear text over the internet. There are all kinds of ways for hackers and crackers to obtain information sent by e-mail. While we will correspond with you by e-mail if that is your preferred method of communication, we want you to understand that this is ***not*** a secure method of exchanging information. Security using e-mail is out of our control.

So what is an alternative to insecure e-mail? We have designed our website at <http://www.argusinsurance.com> so you may register and activate an account which will allow you to securely communicate via a Message Center with members of your Service Team.

What do you mean by "securely communicate"? Our login page, and other pages on our website, uses SSL (secure sockets layer) 128 bit encryption to secure the transmission of data over the internet. SSL is the industry standard ensuring the privacy and security of your data as it passes through the internet. SSL safeguards your data by preventing your login and other information from being intercepted while it is transmitted over the internet.

How can I be sure my data is secure? When you login, the web address or URL's (uniform or universal resource locator) used to access your data are all preceded with "https://" instead of "http://www". This means that a secure connection has been established with our web server. In some browsers, you will see a lock icon in at the bottom of the browser window. Every one of our web pages preceded by the https is a secure page and you can provide the information requested there with confidence.

Why is a secure login so important? Identity theft is on the rise! Keeping your personal information secure should be of vital concern to you. It is to us. We take the responsibility to keep the information you provide as private and confidential. In order to transact business, we do share some of this information with insurance providers on your behalf but that would be the only time.

How does SSL work? An SSL Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key. They can begin a secure session that guarantees message privacy and message integrity.

Without SSL encryption, packets of information travel through networks in full view. Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. Without third-party verification, how do you know a Web site is really a business you trust? Imagine receiving an envelope with no return address and a form asking for your bank account number. An SSL Certificate helps Web site visitors protect sensitive information and get a better idea of who they are trusting with it.

Who provides your SSL Certificate? We use VeriSign. VeriSign is the SSL Certificate provider of choice for over 93% of the Fortune 500, the world's 40 largest banks, and 94% of the top-50 e-commerce sites. Visit the VeriSign web site at <http://www.verisign.com> to learn more about their SSL Certificate and internet security.



ABOUT SSL CERTIFICATES