Security Tips

We care about protecting you from fraud and cybertheft. Please note the following tips to prevent possible electronic fraud:

Phishing attack:

Fraud designed to impersonate a website or an email. Normally an email is received with instructions inviting the user to click on a link. This link takes the user to a fraudulent site where they try to steal your personal data or access to bank accounts.

Secure Title will never ask you for sensitive information such as usernames and/or passwords of applications by email.

Always enter our website by entering the address stla.net in the browser of your choice.

Verify that when entering the STLA site it starts with the prefix https, indicating that it is a secure and authentic page.

Any suspicious situation please report immediately to the mail: **osi@stla.net**

Social Engineering:

Is an attack where malicious people try to pretend to be a Secure Title employee. This attack can be executed in three ways: in person, by email or by phone call. For example, an email is received from **yhernandez@sttla.net** requesting sensitive information or sending false transfer instructions. Note that the domain **sttla.net** does not correspond to the true domain of Secure Title.

When receiving an email, verify that the sender's address contains the correct domain: **stla.net**.

Do not open suspicious or unwanted attachments, these may contain malicious software that could infect your computer.