ONLINE SAFETY RECOMMENDATIONS

Cyberspace is often used to spread electronic messages with hyperlinks to harmful content. Usually they represent malicious attempts to obtain sensitive information such as usernames, passwords, details of credit and debit cards, etc.

ZEAD BULSTRAD VIENNA INSURANCE GROUP does not request from its customers to send via email any personal data or other sensitive information (usernames, access passwords, verification codes, numbers of bank account or bank cards, personal ID numbers or client numbers).

If you have received a suspicious message sent on behalf of BULSTRAD, please notify us by calling 0800 11 111 or through the form under the Contacts section on our website. We advise you to delete the message, without opening any links in it or responding to the sender.

Always access your profile through the Company's website with address: https://www.bulstrad.bg

For the protection of its website Bulstrad uses a certificate with a high security standard, **Extended Validation SSL certificate,** thus preventing fraud or phishing attempts. Users can identify the site's authenticity by the following visual signs (depending on the type of browser used):

- green address bar;
- company name shown in the address bar;
- https:// protocol at the beginning of the URL address;
- closed padlock icon in the address bar;
- information about the organization in the details of the certificate.

Absence of these visual signs may indicate that you have been taken to a false version of the site.

We advise you to always observe the following:

- Use the legal versions of the OS from the official sites of the manufacturer
- Promptly obtain updates and use the newest version of the OS and Internet browser
- Install an antivirus program and update it regularly
- Do not open hyperlinks sent through suspicious emails and do not respond to such messages
- Check preventatively the hyperlinks in received emails [*placing the mouse pointer (WITHOUT CLICKING) over the hyperlink will reveal the linked address*]
- Refrain from downloading or opening atypical attached files or documents
- Be cautious with emails or sites which request personal or financial information which contains: usernames, access passwords, verification codes, numbers of bank accounts or bank cards, personal ID numbers or client numbers
- Do not save your usernames and passwords in the browser
- Do not use the same username and password for accessing different sites and applications
- Change regularly your passwords for accessing Internet sites
- Avoid connecting your mobile devices to public Wi-Fi networks. Unsecured traffic, including sensitive information and identity and access data can intercepted for harmful purposes