ПРЕПОРЪКИ ЗА СИГУРНОСТ

В Интернет пространството се разпространяват имейл съобщения, съдържащи хипервръзки към зловредно съдържание. Обикновено това са злонамерени опити за придобиване на чувствителна информация, като потребителско име и парола, детайли на кредитни и дебитни карти и др.

ЗАД „БУЛСТРАД ВИЕНА ИНШУРЪНС ГРУП“ не изисква да изпращате посредством електронна поща (e-mail) лични данни и друга чувствителна информация (потребителски имена, пароли за достъп, верификационни кодове, номера на банкови сметки или карти, ЕГН или клиентски номер).

В случай, че сте получили съмнително съобщение от името на БУЛСТРАД, моля сигнализирайте ни на номер 0800 11 111 или чрез формата в секция Контакти на сайта, като Ви съветваме да го изтриете без да отваряте съдържащи се в него линкове, както и да не отговаряте на изпращача.

Винаги влизайте в профила си през страницата на Дружеството на адрес: https://www.bulstrad.bg

За защита на уеб сайта си БУЛСТРАД използва сертификат с висок стандарт на сигурност - **Extended Validation SSL certificate** (сертификат с удължена валидация). По този начин се предотвратяват опити за измама или фишинг. Потребителите могат да установят валидността на сайта чрез следните визуални обозначения (в зависимост от използвания браузър):

- зелена адресна лента;
- името на компанията е изписано в адресната лента;
- протокол https:// в началото на URL адреса;
- заключен катинар в адресната лента;
- информация за организацията в детайлите на сертификата.

Липсата им може да означава, че сте попаднали на фалшиво копие на сайта.

Съветваме Ви винаги:

- Да използвате легални версии на операционна система от официалните сайтове на производителя
- Да прилагате навреме актуализациите и да ползвате най-новите версии на операционните системи и интернет браузъри
- Да инсталирате антивирусна програма и да я обновявате редовно
- Да не отваряте хипервръзки, изпратени чрез съмнителни имейли и да не отговаряте на такива съобщения
- Да проверявате хипервръзките в изпратените съобщения [*задръжте мишката (БЕЗ ДА НАТИСКАТЕ) върху хипервръзката и ще разкриете адреса, към който води*]
- Да не сваляте и да не отваряте нетипични прикачени файлове или документи
- Да бъдете внимателни към имейли или сайтове, които изискват лична или финансова информация, която включва: потребителски имена, пароли за достъп, верификационни кодове ,номера на банкови сметки или карти, ЕГН или клиентски номер
- Да не записвате потребителските си имена и пароли в браузъра
- Да не използвате едно и също потребителско име и парола за достъп до различни сайтове и приложения
- Да променяте редовно паролите за достъп до интернет услуги
- Да избягвате свързването на мобилни устройства към обществени Wi-Fi мрежи. Несигурният трафик, включително чувствителна информация и идентификационни данни за влизане, могат да бъдат прихванати от недоброжелател