

* Никогда никому не сообщать реквизиты своих банковских счетов и банковских карт.
* Для осуществления онлайн-платежей использовать только надёжные платёжные сервисы, обязательно проверяя доменное имя ресурса в адресной строке браузера.
* Не хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам.
* Воздерживаться от онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.
* Не перечислять денежные средства на счета электронных кошельков, карт-счета банковских платёжных карточек, счета SIM-карт по просьбе пользователей сети Интернет.
* Для доступа к системам дистанционного банковского обслуживания, электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам использовать сложные пароли, исключающие возможность их подбора.
* При составлении платёжных документов важно проверять платёжные реквизиты получателя денежных средств.
* Не открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров; не переходить по ссылкам в сообщениях о призах и выигрышах.
* Использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять её.
* Ознакомить с перечисленными правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.