



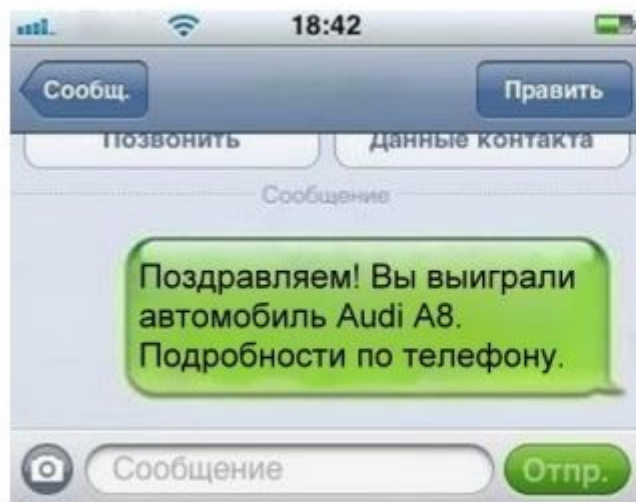
## **ПАМЯТКА для граждан о профилактике и предупреждении дистанционных преступлений в сфере информационно-телекоммуникационных технологий**

### **КЫЗЫЛСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА**

**Чтобы не оказаться жертвой мошенников необходимо знать следующее:**

- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
- ни при каких обстоятельствах не сообщать данные вашей банковской карты, а также секретный код на оборотной стороне карты (CVC);
- хранить ПИН-код отдельно от карты, ни в коем случае не писать ПИН-код на самой банковской карте;
- не сообщать ПИН-код третьим лицам;
- остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;
- лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;
- внимательно читайте СМС-сообщения, приходящие от банка;
- никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС-сообщении от банка;
- помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС-сообщении от банка;
- сотрудники банка никогда не попросят вас пройти к банкомату;
- если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;
- не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;
- никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;
- в сети «Интернет» не переходите по ссылкам на неизвестные сайты;
- действуйте обдуманно, не торопливо, помните, что «Бесплатный сыр только в мышеловке».

## СИТУАЦИЯ 1



Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

**НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.**

*Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.*

## СИТУАЦИЯ 2



Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

**НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.**

*Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнетесь с мошенниками крайне высока.*



### СИТУАЦИЯ 3



Вы получили sms-сообщение о том, что ваша банковская карта заблокирована?

**НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных sms.**

*Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.*

### СИТУАЦИЯ 4



На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

**НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.**

*Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.*

### СИТУАЦИЯ 5

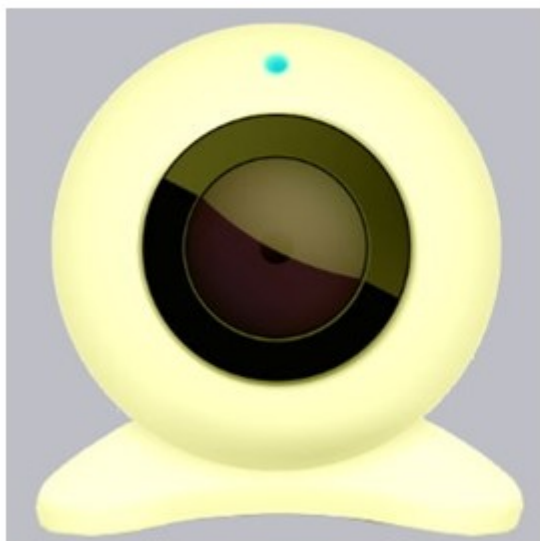


Вы хотите приобрести авиабилеты через Интернет?

**НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.**

*Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.*

### СИТУАЦИЯ 7



Общаетесь в интернете и имеете аккаунты в соцсетях?

**НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.**

*Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.*