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



**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;**

**– не при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;**

**– 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».**

Интернет-мошенничество - памятка для граждан

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего, необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Если вы решили испытать счастье и выйти на связь с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша.

Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или т.н. «электронные кошельки».

Будьте бдительны и помните о том, что для того, чтобы что -то выиграть, необходимо принимать участие в розыгрыше. Все упоминания о том, что ваш номер является «счастливым» и оказался в списке участников лотереи, являются, как правило, лишь уловкой для привлечения вашего внимания.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего - необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату, зачастую путем внесения денежных средств на некий виртуальный кошелек посредством терминала экспресс-оплаты. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

Цель подобных сайтов – обмануть максимальное количество людей за короткий срок. Создать Интернет-сайт сегодня – дело нескольких минут, поэтому вскоре после прекращения работы сайт возродится по другому адресу, с другим дизайном и под другим названием.

Если вы хотите купить товар по предоплате помните, что серьезные Интернет-магазины не будут просить вас перечислить деньги на виртуальный кошелек или счет мобильного телефона. Поищите информацию о магазине в сети Интернет, посмотрите, как долго он находится на рынке. Если вы имеете дело с сайтом крупной или известной вам компании, убедитесь в правильности написания адреса ресурса в адресной строке вашего браузера. При необходимости потребуйте от администраторов магазина предоставить вам информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц. Убедитесь в том, что вы знаете адрес, по которому вы сможете направить претензию в случае, если вы будете недовольны покупкой.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер.

Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что –то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

Если вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто -то из знакомых вам людей, будет не лишним дополнительно убедиться в этом, ведь сообщение могло быть отправлено с зараженного телефона без его ведома. Если отправитель вам не знаком, не открывайте его.

Помните, что установка антивирусного программного обеспечения на мобильное устройство - это не прихоть, а мера позволяющая повысить вашу безопасность.