Как не стать жертвой кибер–мошенников.

Проведенный прокуратурой города анализ поступающих в

правоохранительные органы сообщений о преступлениях свидетельствует, что

интернет-преступники активно используют различные способы завладения

денежными средствами населения.

Стать жертвой мошенника можно не только на улице. С развитием технологий

злоумышленники быстро освоили и виртуальное пространство.

Рассмотрим, какие схемы используются в интернете и как можно обезопасить

себя от кражи.

1. Если вы решили купить товар с рук или продать ненужную вам вещь,

будьте внимательны — мошенники нередко играют роль покупателей или

продавцов. На ваш товар находится крайне заинтересованный покупатель, который

готов перевести аванс на ваш счёт и просит у вас не только номер карты или номер

телефона, но и код проверки подлинности карты (три цифры на обратной стороне).

Такой подход должен вас насторожить — ведь для перевода денег достаточно

знать только номер карты.

Если вы покупаете товар с рук, у вас могут попросить предоплату и сообщить

все данные карты. Если перед вами мошенник, то в лучшем случае вы останетесь

без денег, которые отправили авансом. В худшем — если у вас попросили все

данные карты — рискуете остаться и без средств на счёте.

Как предотвратить?

Будьте осторожны, покупая товары с рук через социальные сети или

специальные сайты. Всегда старайтесь проверить потенциального покупателя или

продавца по отзывам. В сообществах и на сервисах обычно есть «черный список»

(и покупателей, и продавцов) и модераторы. Проверьте профиль продавца — часто

мошенники создают фальшивые страницы с минимумом информации.

2. Ваш друг прислал вам личное сообщение с просьбой одолжить денег или со

странной ссылкой. Это значит лишь одно — аккаунт вашего друга взломали.

3. Незнакомый человек пишет вам личное сообщение, в котором предлагает

стабильный и высокий доход за некую несложную работу. В сообщении нет

конкретной информации, но есть ссылка, по которой вы якобы найдете

подробности. По такой ссылке нет работы мечты — разве что компьютерный

вирус.

4. Часто мошенники представляются сотрудниками известных брендов и

компаний из любых областей. Вам обещают кредиты под низкий процент, большие

скидки, бесплатные товары или говорят, что вы выиграли в конкурсе. Чтобы

получить приз или скидку, от вас требуется всего ничего — сообщить данные

вашей карты, паспорта или все сразу, либо оплатить страховку за пересылку

выигранного подарка.

Как предотвратить?

Если странные сообщения через социальные сети шлёт ваш друг, как можно

скорее позвоните ему и выясните, действительно ли ему нужна помощь. Или

мошенники взломали его аккаунт — и могут обмануть кого-то ещё.

Ссылки из сообщений незнакомцев — не лучший способ искать заработок в

интернете.

Если незнакомцы пишут вам от лица компании или бренда, лучше уточнить

информацию на официальном сайте компании или ее странице в социальной сети

— крупные компании редко проводят конкурсы, в которых вы можете победить,

даже не участвуя, и никогда просто так не запрашивают ваши личные данные,

а тем более данные карты.

5. Мошенники копируют известные сайты, используя похожее название

компании и оформление. Например, вы хотите узнать, есть ли у вас штрафы в

ГИБДД или как оформить кредит онлайн, а попадаете на фишинговый сайт, то есть

сайт-клон. Если вы введёте на таких сайтах свои данные, они попадут в руки

злоумышленников.

Как предотвратить?

Всегда обращайте внимание на адресную строку браузера: на сайте-клоне

будет допущена ошибка. Оплачивайте покупки только через сайты с защищённым

соединением и значком платёжной системы. Внимательно изучите и содержание

сайта — злоумышленники часто невнимательно относятся к наполнению сайта.

Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать

адрес вручную — так вы не ошибётесь в названии и попадёте на нужный вам сайт.

6. Зловредные программы умеют маскироваться под мобильные банки и

таиться в разных приложениях, которые вы скачиваете на телефон.

Скачивайте приложения на телефон только в официальном магазине.

Обращайте внимание в первую очередь на разработчика приложения — в

официальных банковских приложениях указан сам банк. Внимательно читайте

описание приложения. Не скачивайте приложения сторонних разработчиков.

Соблюдение приведенных правил может обезопасить вас от кибер-

мошенников и сохранить Ваши денежные средства.