

Как не стать жертвой мошенников, которые используют информационно-телекоммуникационную сеть «Интернет»

С развитием технологий значительно возросла доля различных проявлений мошенничеств в телекоммуникационной среде, совершаемых посредством телефонных звонков и в сети «Интернет».

Вместе с тем, и давно известные способы хищения продолжают использоваться злоумышленниками.

Оградить от мошенников в первую очередь способны знания, внимательность, здравомыслие и критическая оценка ситуации. Поможет и знание типичных «схем» работы мошенников и соблюдение правил, изложенных в данной статье.

Покупка в интернет-магазине мошенника.

Покупки в интернете в последние годы приобрели значительную популярность и получили доверие со стороны граждан, чем и пользуются мошенники.

Создать интернет-магазин и наполнить его фотографиями товаров, которые якобы есть у продавца в наличии – дело нескольких минут. После того как деньги за товар будут отправлены (такие интернет-магазины обязательно требуют предоплату), сотрудники магазина перестанут выходить на связь, либо придумывать отговорки, а потом магазин бесследно исчезнет.

Вскоре после прекращения работы сайт может возродиться по другому адресу, с другим дизайном и под другим названием, ожидая очередных доверчивых клиентов.

Как обезопасить себя? Никогда не совершайте покупки в непроверенных интернет-магазинах, особенно если требуется внесение предоплаты. Уточните юридический адрес организации и проверьте через интернет существует ли такая организация в действительности, позвоните в неё чтобы убедиться в том, что это действительно интернет-магазин.

Сайты-двойники.

Один из способов кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации – создание сайтов-двойников. Внешне такие сайты не отличаются от оригинальных, разница как правило лишь в одной букве адреса.

Если невнимательный пользователь не заметит разницы и введет свои логин и пароль на таком сайте, то эти данные окажутся в руках злоумышленника.

Как обезопасить себя? Обращайте внимание на правильность написания адреса сайта, а также же на показатели безопасности сайта, такие как значок закрытого замка в адресной строке браузера и наличие буквы «s» (обозначает «secure» – безопасный), «https://» в начале адреса сайта. Если эти элементы отсутствуют – на такой странице небезопасно вводить данные, особенно реквизиты банковских карт.