**Основные виды кибермошенничества**

«Выгодные» покупки в социальных сетях». Дешевый товар, аренда квартиры с предоплатой, покупка билетов «онлайн» и т.д. При данном виде мошенничества продавец будет сообщать, что Вы такой не единственный и уже вот-вот придет покупатель, но, чтобы Вы стали первым в очереди, необходимо внести предоплату. Удержитесь от соблазна легко заработать или значительно сэкономить, и не переводите деньги незнакомцам или сомнительным предпринимателям, а встречайтесь в живую либо используйте проверенные способы пересылки (почта, европочта с наложенным платежом и т.д.), даже если у продавца будет хороший рейтинг либо хорошие отзывы. Зачастую сами страницы являются «фэйковыми».

«Инвестирование средств в биржи для получения прибыли». Мошенники завлекают лиц. особенно не владеющими определенными познаниями в данной области. при этом убеждают, что все работает, переведя на счет потерпевших незначительную сумму в качестве прибыли. Потерпевший после этого доверяет злоумышленнику и переводит на подконтрольный счет последнего имеющиеся у него денежные средства.

СМС-рассылки о выигрышах и бонусах, реклама на Интернет площадках о выигрышах, интернет-опрос, в которых в последующем предлагается заплатить комиссию за банковский перевод, указать реквизиты банковских, карт для получения выигрыша или что-то подобное.

Опасные знакомства. Мошенники умело манипулируют чувствами людей, в основном ведя переписку длительное время в социальных сетях, однако со временем попросят деньги, например, на подготовку свидания, на срочное лечение ребенка или даже на совместный поход в кино. Не нужно поддаваться эмоциям, лучше встретится в живую и убедится в личности человека. Ну а если собеседник избегает личных встреч, то это наверняка мошенник.

«Звонок из банка», из Следственного комитета, милиции. Зачастую мошенники звонят посредством «VIBER», сообщая, что на вас кто-то оформил кредит и нужно перевести деньги на безопасный счет, иногда просят установить на телефон приложение по направленной ссылке. Если такие факты возникли - это мошенник. Сотрудники банка и сотрудники правоохранительных органов не звонят на «Viber», даже если в вашем телефоне определился официальный номер банка, изображение банка, правоохранительного органа.

«Несчастье» с близкими. Мошенники манипулируют жертвами, заставляя поверить, что их близкие люди якобы оказались в чрезвычайной ситуации, звоня по мобильному и городскому телефону, в основном от правоохранительных органов, когда на заднем плане слышен якобы голос родственника о помощи. В стрессовой ситуации человек отдает деньги, чтобы помочь в случае аварии, кражи денег, срочных медицинских расходов, требования взятки и т.д., за которыми в основном приезжает курьер. В данном случае необходимо прервать разговор с собеседником и побыстрее связаться с пострадавшим родственником, какой бы драматичной ни была рассказанная вам история. С недавнего времени, для придания правдивости преступники с использованием искусственного интеллекта стали звонить голосами близких и родных.

Фишинг. Под предлогом покупки какого-либо у Вас товара и перевода за него денежных средств, объявление о котором размещено на какой-либо интернет площадке, предоставляют ссылку, по которой Вы переходите на фишинговый сайт, после чего в соответствующие поля предлагают ввести реквизиты БПК для получения средств за товар, однако мошенники тем самым получают доступ к Вашему счету и списывают с него средств

*Звонок* от руководителя организации, предприятия. Мошенники от имени руководителей учреждений и предприятий, используя реальные данные людей и их рабочие контакты (которые не сложно получить в сети Интернет) выходят на связь с подчиненными работниками. Мошенники создают в мессенджерах поддельные аккаунты, с реальной фотографией и фамилией руководителя (иногда взламывают аккаунт). Далее выдавая себя за руководителя, мошенник списываются с подчиненным через мессенджер и предупреждает о предстоящем разговоре с сотрудником КГБ (МВД, СK, КГК) и призывают оказать ему всяческое содействие и выполнить то, что он скажет.

Кибервымогательство iCloud IPhone, в ходе которого злоумышленники знакомятся в социальных сетях, потом под предлогом того, что не могут зайти в свой iCloud IPhone по различным причинам, просят войти в их iCloud для доступа к якобы ценной информации, при доступе к которому меняют логины (пароли) и Вы не сможете снова войти в свое устройство, а для разблокировки устройства требуют передачи средств.

Звонки от работников А1, МТС. Мошенники звонят и представляются сотрудниками А1, МТС, спрашивают, удовлетворены ли Вы работой сотовой связи, после чего сообщают об устаревшим приложении и просят установить новое приложения сотового оператора, после установки которого злоумышленник удаленно получает доступ к Вашему мобильному телефону и управляет им.

Для предотвращения фактов мошенничества не следует по просьбе неизвестных лиц, даже если они представились сотрудниками правоохранительных органов и банков, переводить денежные средства, сообщать какие-либо личные данные, скачивать файлы по их просьбе, переходить по неизвестным ссылкам.