**Профилактика киберпреступлений, информирование граждан**

**об актуальных способах совершения киберпреступлений, устранение причин и условий, им способствующих**

В настоящее время в структуре киберпреступлений, совершенных на территории города Жодино, преобладают преступления, предусмотренные ст. 209 Уголовного Кодекса Республики Беларусь (Мошенничество), которые совершаются под предлогом продажи товаров, оказания услуг в сети Интернет. Также регистрируются преступления под предлогом участия в биржевой торговле, торговле криптовалютой, заработка в сети Интернет, под предлогом оказания финансовой помощи, получения денежных средств в долг, под предлогом осуществления правоохранительной деятельности, обеспечения сохранности денежных средств, персональных данных и иные.

Наиболее популярные виды мошеннических действий в настоящий момент:

1. Продление/перезаключение договора УП «А1», СООО «МТС», «Белтелеком», «Водоканал» и иных организаций. Гражданам звонят через мессенджеры (WhatsApp, Viber, Telegram и иные мессенджеры) и представляются сотрудниками вышеуказанных организаций, под предлогом необходимости продления договора, просят предоставить свои паспортные данные, в том числе идентификационный номер. Зачастую мошенники подталкивают граждан установить или переустановить приложение на свой смартфон, причем присылают ссылку либо же сам установочный файл в личные сообщения. После установки (обновления) уже вредоносного приложения смартфон становится подконтрольным злоумышленнику, после чего у него появляется доступ к данным пользователя, которые хранятся на смартфоне. В результате этого у злоумышленника появляется возможность устанавливать сторонние приложения, оформлять банковские и иные сервисы и услуги. В случае, если вы попались на данную уловку и установили подобное приложение, незамедлительно переведите свой мобильный телефон в режим полета.
2. Аренда квартир с предоплатой. Мошенники убеждают потенциальную жертву в том, что на эту квартиру уже образовалась очередь и вынуждают произвести предоплату на предоставленную БПК, счет, криптокошелек и другое. Примечательно, что злоумышленники чаще всего созваниваются и ведут переписки не по сотовой связи, а посредством различных мессенджеров.
3. Покупка товаров в социальных сетях, социальной сети «Instagram», в мессенджере «Telegram» и других. Злоумышленники активно используют данные инструменты для завлечения «клиентов». Для достижения своих целей злоумышленники выставляют цену на продаваемые товары значительно ниже рыночной. Аккаунты выглядят «живыми»: красивые видео, картинки, большой выбор товаров, множество сторисов, большое количество подписчиков. Вместе с тем их условия следующие: полная или частичная предоплата без возможности произвести оплату по факту получения товара. Товар же предлагают отправить либо курьером, либо по почте. Наиболее популярные темы вышеуказанных аккаунтов: продажа автомобильных шин, морепродуктов, цветов, туристических курортов, новогодних подарков, елок, мобильных телефонов (преимущественно фирмы «Apple»), детских вещей, курток, колясок и иное.
4. «Выигрыши» подарков, призов, которые Вам готовы отправить различными службами доставки. Злоумышленники пользуются доверием и снижением бдительности граждан. Единственным условием для Вас со стороны злоумышленников является то, что Вам необходимо оплатить пересылку, после чего Вы сами того не понимая предоставляете под каким-либо предлогом свои данные, либо же доступ к своим данным, в результате чего денежные средства переводятся на мошеннические счета.
5. Сайты знакомств. Злоумышленники активно общаются с жертвой, созваниваются в мессенджерах, активно интересуются жизнью, максимально входят в зону доверия, после чего в подходящий момент просят одолжить денежные средства для каких-либо целей, либо же предлагают вложить свои сбережения в какой-либо «выгодный» проект, акции, криптовалюту и иное, аргументируя это тем, что сами зарабатывают таким образом.
6. При покупке/продаже товаров на торговой площадке «Kufar» злоумышленники интересуются опубликованным товаром, в результате чего предлагают приобрести товар с помощью службы доставки (как правило «Куфар доставка» либо «Автолайт»), либо при помощи отправки почтой, после чего предоставляют фишинговую ссылку, которая ведет на Интернет-ресурс внешне идентичный официальному ресурсу службы доставки, либо почтовой связи, в результате чего после ввода своих персональных данных либо данных банковской платежной карты, мошенники завладевают денежными средствами, находящимися на карт-счетах жертвы.
7. Просьбы «знакомых» в социальных сетях, мессенджерах о перечислении денежных средств в долг. Не перечисляйте денежные средства своим знакомым до тех пор, пока не созвонитесь лично и не убедитесь в действительности данной просьбы, так как зачастую учетная запись оказывается «взломанной», а общение ведется злоумышленниками.
8. «Алло мама». Злоумышленники звонят в мессенджерах, на домашний телефон, мобильный телефон, притворяясь вашей дочерью, сыном, внуком, внучкой и истерично, зачастую голосом, похожим на голос Ваших родных говорят, что они якобы попали в аварию, либо же сбили человека и им нужны денежные средства чтобы «замять» дело. В случае если Вы попали в подобную ситуацию, рекомендуется немедленно прервать звонок и позвонить Вашим близким, от имени которых поступал звонок.
9. Злоумышленники зачастую представляются сотрудниками правоохранительных органов и под различными предлогами пытаются Вас убедить перевести все свои накопленные денежные средства на предоставленные ими счета якобы с целью поимки преступников. Зачастую данные действия также проходят под угрозой проведения обыска по Вашему месту жительства, во время проведения которого будут изъяты все сбережения, именно поэтому и необходимо их «задекларировать» либо «перевести на безопасный счет».
10. Реклама в различных социальных сетях о вложении в акции различных компаний, таких как «Tesla», «Apple» и иных, с целью получения дивидендов.
11. Предложения о подработке, в результате чего злоумышленники убеждают предоставлять свои персональные данные, открывать банковские счета, а также устанавливать различные подозрительные приложения. Зачастую, под предложением таковых подработок маскируется содействие злоумышленникам в переводах похищенных денежных средств иных граждан, которые потенциальный «работник» принимает на свои банковские платежные карты, а в дальнейшем переводит по указанным «работодателем» реквизитам.
12. Просьбы проголосовать в какой-либо социальной сети или мессенджере за дочь, внучку, знакомого. Таким образом, Вы сами не зная того, предоставляете злоумышленникам доступ к Вашим учетным записям мессенджеров, как правило мессенджера «Telegram», «Viber» либо «WhatsApp».

***При совершении любых из приведенных преступлений, злоумышленниками могут использоваться***:

- поддельные фотографии банковских карт (с измененными номерами, именем держателя, банка эмитента и т.д.);

- поддельные (созданные с использованием возможностей искусственного интеллекта) аудио записи (голосовые сообщения), в том числе схожие с голосом родственников жертвы, для наибольшей степени воздействия;

- в момент совершения преступления злоумышленником могут использоваться видеовызовы, во время которых применяются возможности искусственного интеллекта и подменяется передаваемое изображение (применение маски лица на говорящем, для визуальной схожести с государственными служащими), в также обстановка и предметы интерьера, для создания впечатления о нахождении преступника в настоящем кабинете государственных органов (изображение государственных символов Республики Беларусь, портреты главы государства и иное).

Помните, что настоящие сотрудники правоохранительных органов не ведут общение посредством мессенджеров, в том числе с использованием видеосвязи и не требуют осуществления каких-либо действий на Вашем мобильном устройстве!