**Кибербезопасность: новые виды**

**и формы мошеннических киберугроз**

 Интернет стал настолько привычной частью нашей жизни, что иногда мы забываем, что не все, с кем мы общаемся онлайн, являются порядочными людьми. Киберпреступления в наши дни являются одним из самых распространенных методов обмана граждан. Данный вид преступлений никогда не стоит на месте. Лучший способ защиты от онлайн-мошенников – знать о рисках и уметь их избегать.

В Молодечненском РОВД с начала года зарегистрировано больше сотни преступлений, связанных с хищением денежных средств, из них 69 – мошенничество. Исходя из анализа совершенных преступлений установлено, что у жителей города Молодечно было похищено более 500.000 рублей.
 *Наиболее распространенными схемами обмана на данный момент являются:*

- сообщение от якобы «руководителя» фирмы, который уведомляет работника о том, что с ним хотят поговорить сотрудники банка/налоговой/правоохранительных органов. Собеседник задает вам вопросы, касаемо вашей работы, а в конце разговора просит сказать цифры, которые приходят на мобильный телефон. Итог один – потеря денежных средств с банковской карты.

- покупка автомобилей, мобильных телефонов и прочих гаджетов. Вы связываетесь с продавцом, который просит у вас предоплату за товар. Даже самый популярный сайт или аккаунт с хвалебными отзывами не защищает вас от мошеннических действий. Такие истории, как правило, заканчиваются одним – вы перечисляете предоплату, а связь с продавцом теряете, не получив долгожданный товар.

- мошенничества с пластиковыми картами. Вам приходит сообщение о том, что ваша банковская карта заблокирована и предлагается бесплатно позвонить на определенный номер для получения подробной информации, не торопитесь звонить по указанному телефону. Чтобы похитить ваши денежные средства, злоумышленникам нужен номер вашей карты и ПИН- код, для этого они могут сказать о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. Как только вы их сообщите, деньги будут сняты с Вашего счета.

- вымогательство. «Интернет-друзья» не всегда являются теми людьми, за которых вы их принимаете. Отправляя какие-либо фотографии или информацию, граждане часто сталкиваются с неприятной ситуацией: с них требуют деньги за «молчание».

- звонок от оператора сотовой связи. Суть проста: вам звонит якобы оператор сотовой связи и сообщает, что ваш договор с ними скоро заканчивается. Далее, просит вас зайти на предоставленный сайт, внести персональную информацию и сообщить код, который придет на мобильный телефон. Так ваши денежные средства и переходят мошенникам, оставляя вас ни с чем.

*Огородить себя от преступных посягательств можно только путем соблюдения нескольких простых правил:*

- никому и никогда не сообщайте подробную информацию о своей банковской карте. Пин-код, кодовое слово, CVV (или CVC2), код 3D-Secure и полученные от банка одноразовые пароли должен знать только владелец карточки.

- если информация о карточке хранится в смартфоне или планшете, не следует читать сообщения, пришедшие с неизвестных номеров, и ни в коем случае не открывать ссылки в них.

- при использовании известных вам сайтов, обращайте внимание на их внешний вид: возможно, вы зашли на поддельную ссылку. Как правило, мошеннические ссылки имеют окончание «com».

**Избегайте любых предоплат!**

**С осторожностью относитесь к письмам, в которых запрашиваются данные счетов!!!**

*Помните, что сотрудники правоохранительных органов, налоговой службы или банка никогда не звонят через мессенджеры, и уж тем более не просят вас сообщить коды из СМС. Будьте внимательны!!!!*