**Киберпереступление**

Развитие интернет-технологий - это не только плюсы. Существенным минусом такого развития является все большее распространение так называемых киберпреступлений (то есть преступлений в интернет-пространстве). Что нужно знать, чтобы обезопасить себя от постороннего вторжения.

 У современного человека, как правило, имеется в наличии не один гаджет. Это и мобильный телефон, и ноутбук, и разнообразные айпады/айподы и др. С помощью этих устройств человек осуществляет поиск информации в сети Интернет, общается в социальных сетях, совершает покупки и многое другое. Какие-то операции доступны просто так, для других нужна регистрация, для третьих потребуются данные банковской карточки. Логично, что такую информацию, как логины, пароли, номера карт, необходимо защитить и не допустить ее утечки и распространения.

 Необходимо помнить о том, что вмешательство в личную жизнь незаконно, а право на защиту от такого вмешательства гарантировано ст.28 Конституции Республики Беларусь. Об обеспечении неприкосновенности частной жизни при использовании Интернета говорит также и международное законодательство (абз. 8 ст. 5 постановления Межпарламентской Ассамблеи государств - участников СНГ «Об основах регулирования Интернета»). Но в реальности такое вмешательство происходит довольно часто.

С начала 2019 года на территории Кормянского района возбуждено 7 уголовных дел по факту хищений путём использования компьютерных технологий и сопряжённых с обманом пользователей сети Интернет, а также 4 уголовных дела за несанкционированный доступ к компьютерной информации. К примеру за аналогичный период 2018 года в пределах района не зарегистрировано ни одного преступления из указанной категории.

 Тенденция к росту киберпреступности характерна не только для Кормянского района, но и для всей Республики. Большинство таких преступлений связано со взломом страниц пользователей социальных сетей, благодаря чему преступники под каким-либо предлогом получают денежные средства потерпевших или доступ к их банковским счетам.

 Несмотря на проделанную работу профилактического характера в части просвещения граждан о способах защиты от преступлений путём использования компьютерных технологий, также преступления по-прежнему совершаются в отношении жителей Кормянского района.

 Так, в августе 2019 года неустановленное лицо, имея умысел на хищение денежных средств, используя глобальную компьютерную сеть «Интернет», в социальной сети «ВКонтакте», завладев сведениями о реквизитах банковской пластиковой карты ОАО «Беларусбанк», эмитированной на имя жителя г.п.Корма Н., получило доступ к компьютерной информации – карт-счету указанного лица, после чего, путем незаконной транзакции, совершило хищение денежных средств, на сумму 60 рублей. Злоумышленник, используя в своих преступных целях взломанный аккаунт одного из знакомых потерпевшего, в ходе переписки ввёл последнего в заблуждение о необходимости перечисления денежных средств на банковский счёт, получив доступ к карт-счету гражданина Н., после чего совершил хищение.

 При необходимой доле бдительности и осмотрительности, потерпевший мог бы предотвратить преступные действия злоумышленников, однако пренебрёг самыми простыми правилами использования сети интернет.

 Основными признаками мошенничества в Интернете являются:

- навязчивая реклама, обещающая огромных доход без вложений;

- «заманчивые» предложения, поступающие на электронный ящик или в социальной сети от незнакомых людей;

- требование ввода ваших персональных данных, а также отправки СМС на сомнительных ресурсах;

- требование предоплаты за товар (услугу) на сомнительных (непроверенных) ресурсах;

- просьбы от знакомых в социальных сетях о предоставлении данных банковской карты под различными предлогами (личная страница пользователя может быть взломана);

- эмоциональное сближение с собеседником (как правило, иностранным гражданином), если в конечном итоге переписка сводится к просьбе одалживания денег под любым предлогом и др.

 Несмотря на то что уровень знаний киберпреступников в соответствующей области достаточно высок, мнимизировать риск вмешательства вполне возможно, придерживаясь следующего:

1. не переходите по сомнительным ссылкам из писем сообщений или СМС;
2. устанавливайте приложения только из официальных источников;
3. не сообщайте никому свои пароли, логины, реквизиты банковских карт и прочие данные, с помощью которых можно получить доступ к внешней личной информации

Не безопасно также давать свой телефон постороннему человеку для звонка. Некоторые операторы мобильной связи предоставляют услугу микрозаймов, активировать которую можно с помощью USSD-кода. Этим и может воспользоваться недобросовестный незнакомец.

Абсолютной за щиты от противоправных действий злоумышленников на просторах Интернета нет. Однако, придерживаясь хотя бы вышеуказанных рекомендаций, можно минимизировать попытки вмешательства посторонних лиц из вне с целью завладения информации, представляющих для последних особый интерес.

Помощник прокурора

Кормянского района Савичев Д.А.