**Преступления в социальных сетях: какие правила необходимо соблюдать для защиты личной информации**

**В мире неуклонного развития высоких технологий большинство из нас не может себя мыслить без гаджетов и глобальной сети Интернет. Практически у всех есть страница в социальных сетях, электронные почтовые ящики, Viber. В Интернете, на компьютерах мы храним наши персональные данные. Однако мало кто из нас задумывается, что электронные средства хранения более уязвимы, чем бумажные. Размещаемые посредством электронных средств хранения данные можно и уничтожить, и скопировать, и незаметно видоизменить.**



Как показывает практика, одним из способов совершения данного преступления является несанкционированный доступ к страницам пользователей в социальной сети «Вконтакте». Злоумышленник под аккаунтом пользователя сети, ничего не подозревающего, с целью получения корыстной выгоды рассылает сообщения его знакомым и друзьям.

Например, при взломе страницы в социальной сети «Вконтакте» гражданина П. злоумышленник рассылал сообщения его друзьям с просьбой перевести денежные средства на абонентские номера компании связи, зарегистрированной в Российской Федерации. При этом в сообщениях от его имени он написал, что находится в трудной жизненной ситуации и ему в срочном порядке требуются деньги. Друзья пользователя сети, предполагая, что оказывают помощь гражданину П., перевели денежные средства на указанные злоумышленником номера абонентов мобильной сети.

В данном случае произошло совершение сразу нескольких преступлений, а именно по ч.2 ст.349 УК Республики Беларусь (несанкционированный доступ к компьютерной информации, совершенный из корыстной заинтересованности) по отношении к гражданину П., и по ст. 209 (мошенничество) УК Республики Беларусь по отношению к лицам, перечислившим денежные средства на указанные абонентские номера.

Еще один из распространенных примеров. Неизвестное лицо «взломало» страницу в социальной сети «Вконтакте» гражданина Ф. Воспользовавшись его аккаунтом, от его имени переслало сообщения зарегистрированным в сети его друзьям и знакомым с просьбой указать реквизиты своих банковских карт. Злоумышленник, при пересылке сообщений пользовался данными, хранящимися на странице в социальной сети, а именно использовал способ переписки, словесные обороты, жизненные события, отраженные в предыдущих сообщениях гражданина Ф. и его друзей.

Злоумышленник совершил несколько преступлений – предусмотренное ч.2 ст.349 УК Республики Беларусь по отношению к гражданину Ф. и ч.2 ст.212 (хищение имущества путем введения в компьютерную систему ложной информации, сопряженное с несанкционированным доступом к компьютерной информации) УК Республики Беларусь по отношению к тем лицам, которые указали реквизиты своих банковских карточек, и с карт-счетов которых были похищены денежные средства.

Чтобы оградить себя от хищений денежных средств, совершенных вышеуказанными способами, необходимо в первую очередь соблюдать правило – не указывать свои персональные данные, реквизиты банковских карточек, логины, пароли и иную конфиденциальную информацию в глобальной сети Интернет.

С целью недопущения несанкционированного доступа к компьютерной информации, необходимо защитить установленный пароль. Следует помнить: нельзя делиться своим паролем; для создания пароля нужно использовать строчные и прописные буквы в вперемешку с цифрами, либо позволить компьютеру самому сгенерировать пароль; предпочтительно использовать длинные пароли, так как они более безопасны; не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным; пароль не должен отображаться на экране компьютера при его вводе; пароли должны отсутствовать в распечатках; нельзя записывать пароли на столе, стене ином видном месте, его нужно держать в памяти.

Соблюдая вышеуказанные правила компьютерной безопасности, Вы сможете оградить себя от преступных посягательств, убережете конфиденциальность персональных данных и свое имущество.

Первый заместитель начальника

ОВД Глусского райисполкома

Хотянович В.Н.