**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.



Число преступлений против информационной безопасности растет. К примеру, в г. Гомеле в текущем году по сравнению с прошлым число преступлений, предусмотренных ст. 349 (несанкционированный доступ к компьютерной информации) Уголовного кодекса Республики Беларусь, по сравнению с 2016 годом выросло на 13 процентов. За 11 месяцев 2016 года в областном центре зарегистрировано 93 таковых преступления, за аналогичный период 2017 года – 105 преступлений.

Как показывает практика, одним из способов совершения данного преступления является «взлом» страниц 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» гражданки Т. злоумышленник рассылал сообщения ее друзьям с просьбой перевести денежные средства на абонентские номера компании связи, зарегистрированной в Российской Федерации. При этом в сообщениях от ее имени он написал, что она находится в трудной жизненной ситуации и ей в срочном порядке требуются деньги. Друзья пользователя сети, предполагая, что оказывают помощь гражданке Т., 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 гражданке Т., 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 Я. 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 Я. и его друзей.

Злоумышленник совершил несколько преступлений – предусмотренное ч.2 ст.349 УК Республики Беларусь по отношению к гражданину Я. 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.

**Справочно**

**Статья 349 УК Республики Беларусь**. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, – наказывается штрафом или арестом.
2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.
3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, – наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

*По сообщению* [*официального сайта Следственного комитета Республики Беларусь*](http://sk.gov.by/)