***Преступления в сети***

Сегодня, многие из нас, пользуются Интернетом - практически у всех есть страница в социальных сетях, электронные почтовые ящики. В Интернете 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. Из года в год количество преступлений, совершенных с использованием компьютерных технологий, неизменно растет.

Значительное увеличение указанных преступлений связано и с ростом несанкционированных доступов к личным страницам граждан в социальных сетях, а также к аккаунтам в мессенджерах, вследствие чего злоумышленники, используя методы социальной инженерии, получают у знакомых владельцев страниц и аккаунтов реквизиты банковских платежных карт, с которых в последующем совершаются хищения денежных средств.

Так, злоумышленник под аккаунтом ничего не подозревающего пользователя сети, с целью получения корыстной выгоды рассылает сообщения его знакомым и друзьям.

Например, при взломе страницы в социальной сети «Вконтакте» гражданина А. злоумышленник разослал сообщения его друзьям с просьбой перевести денежные средства на банковскую платёжную карту, зарегистрированную в Российской Федерации. 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 А., перевели денежные средства на указанную злоумышленником банковскую платёжную карту. Сам гражданин А. при этом находился по месту жительства, и никто из его товарищей не догадался позвонить ему и спросить, что же с ним случилось.

В другом случае, злоумышленник, осуществив несанкционированный доступ в мессенджере «Viber» гражданки В. и воспользовавшись ее аккаунтом, от ее имени переслал сообщения зарегистрированным в сети ее друзьям, содержащие «фишинговые ссылки». Перейдя по данным ссылкам, пользователи мессенджера «Viber» проходили опрос, тем самым принимали участия в «акции». В результате пройденного опроса, друзья гражданки В. ввели реквизиты своих БПК, с целью получения вознаграждения за участие в «акции», однако после данных действий они лишились денежных средств. Стоит обратить внимание, что злоумышленник, при отправлении сообщений, содержащих «фишинговые ссылки», пользовался данными, хранящимися в чатах, а именно использовал способ переписки, словесные обороты, жизненные события, отраженные в предыдущих сообщениях гражданки В. и ее друзей.

Чтобы избежать подобного рода хищений, необходимо в первую очередь соблюдать правило – не указывать свои персональные данные, реквизиты банковских карточек, логины, пароли и иную конфиденциальную информацию в глобальной сети Интернет, а также не переходить по «фишинговым ссылкам» и не сообщать sms-пароли.

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 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.

Старший инспектор ООПП

майор милиции Ковалев А.И.