**КАК НЕ СТАТЬ «ЖЕРТВОЙ» ЗЛОУМЫШЛЕННИКОВ В ИНТЕРНЕТЕ**

В настоящее время на территории Гродненской области фиксируется существенное количество регистрируемых фактов совершения несанкционированных доступов к учетным записям в социальных сетях и к электронным почтовым ящикам с последующим выманиванием у собеседников владельца учетной записи от его имени реквизитов банковских платежных карточек для дальнейшего осуществления транзакций по ним (перечисление на абонентские счета мобильных телефонов, кошельки в электронных платежных системах WebMoney, Яндекс Деньги и т.д.) либо склонением собеседников к осуществлению таких транзакций лично. Такие преступления выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы, имеет возможность ознакомиться с ее содержимым, изучить список контактов, с которыми жертва поддерживает отношения. Зачастую преступник осуществляет смену пароля доступа к учетной записи, тем самым блокирует доступ законному владельцу к аккаунту. Далее злоумышленник осуществляет рассылку всем либо избранным контактам владельца взломанной учетной записи сообщения мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

* «Вася (*к примеру*), я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (*здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах Яндекс.Деньги, QIWI, WebMoney или других*) 5 000 (*мошенник имел ввиду российских, знал бы он, что в Беларуси указанная сумма столь существенна, он бы уточнил*) рублей. Все верну по приезду.»;
* «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом отдашь мне. В долгу не останусь!»;
* «Я помогаю в сборе средств для лечения моей дальней родственницы, у нее серьезная болезнь, нужно много денег. Перечисли, если есть возможность, хоть какую-то сумму на кошелек».

Отметим, что выше описанные действия составляют диспозицию таких статей Уголовного кодекса Республики Беларусь, как:

* 349 «Несанкционированный доступ к компьютерной информации» (в данном случае предусмотрено максимальное наказание до двух лет лишения свободы);
* 350 «Модификация компьютерной информации» (до трех лет лишения свободы);
* 351 «Компьютерный саботаж» (лишение свободы на срок от одного года до пяти лет).

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной

В Гродненской области за 7 месяцев 2018 года по линии информационной безопасности зарегистрировано 143 (+6 к аналогичному периоду прошлого года) преступлений, 103 (+16) из них - хищения с использованием банковских платежных карточек и их реквизитов, 40 – иные преступления, предусмотренные главой 31 Уголовного кодекса Республики Беларусь.

Чтобы не стать «жертвой» злоумышленников помните: реквизиты Вашей банковской карточки опасно передавать третьим лицам по открытым каналам связи, различного рода просьбы перечислить денежные средства на незнакомые номера, кошельки по вымышленным причинам должны восприниматься критично и всегда подтверждаться живым общением с Вашим собеседником. Уделяйте больше внимания безопасности в социальных сетях. Значительного внимания требует обеспечение безопасности доступа к Вашим учетным записям: устанавливайте сложные пароли, периодически их меняйте, пользуйтесь технологией двухфакторной аутентификации.

В случае совершения в отношении Вас аналогичных противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства. Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!

Вриод начальника Слонимского РОВД

подполковник милиции В.М. Осоцкий