Кибербезопасность и профилактика киберпреступности

Виды мошенничеств

В последнее время отмечается рост количества фактов совершения противоправных деяний в сети Интернет. 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.

Злоумышленники получают доступ к личным страницам граждан и от их имени рассылают сообщения виртуальным друзьям. У них мошенники просят о помощи в получении денежного перевода и просят предоставить реквизиты банковской платежной карты (номер карты, срок действия и CVV-код).

**СХЕМА № 1** Схема мошенничества проста, потерпевшему с учетной записи знакомого приходит сообщение с просьбой оказать помощь в получении денежного перевода, пополнении баланса мобильного телефона и иной финансовой помощи. Ссылаясь на различные причины, связанные с неработоспособностью платежной карты либо отсутствием доступа к услугам интернет-банкинга, мошенники просят предоставить реквизиты платежной банковской карты. Достаточно даже фотографии банковской карты с двух сторон.

Всё вышеуказанное образует состав преступления статей Уголовного кодекса Республики Беларусь: ст.349 «Несанкционированный доступ к компьютерной информации», ст.350 «Модификация компьютерной информации» и ст.351 «Компьютерный саботаж».

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 УК Республики Беларусь «Мошенничество».

**СХЕМА № 2** Распространены случаи, когда пользователю, разместившему объявления о продаже имущества на торговых интернет-площадках, например «Куфар», поступают сообщения о желании приобрести имущество, после чего покупатель (злоумышленник) переводит беседу в другой мессенджер *(в сообщениях «Куфар» запрещено сбрасывать ссылки)*, например «VIBER». Мошенник в вайбере предлагает оформить покупку через «Куфар Доставку», вещь забирает курьер, а мошенник под видом покупателя переведет деньги на карту. Такая услуга на «Куфаре» действительно есть. Если человек соглашается, то злоумышленник сбрасывает ссылку на фейковую страницу где необходимо прописать все реквизиты банковской карты, а затем и код-подтверждения «для получения денежных средств». После чего у граждан с карт списываются деньги.

**СХЕМА № 3** На Ваш номер телефона поступает звонок от «сотрудника банка»(МВД, Следственный комитет) в ходе которого он сообщает о том, что по вашей карте происходят мошеннические операции либо по вашему счету оформлена заявка на кредит. На что предлагает установить приложение для того, чтобы обезопасить ее либо заблокировать карту, однако для блокировки необходимо подтвердить свою личность для этого начинает расспрашивать Вас о реквизитах карты, так же может спросить идентификационный номер паспорта (**НИ В КОЕМ СЛУЧАЕ НЕ СООБЩАТЬ**), после чего для самой блокировки просит сообщить код из SMS-сообщения. **(Это «Вишинг», в подобных случаях очень трудно понять, что**

**ники банка никогда не спросят код из SMS-сообщений, СVV-код (3-ёх значное число с обратной стороны карты), ПИН-код от карты, а так же никогда не попросят установить что-либо из интернета себе на мобильный телефон)**.

**СХЕМА № 4** заключается в том, что при использовании интернет-банкинга, жертва заходит в браузер и вбивает в поисковую строку «Интернет -банкинг», после чего ей предоставляется 4 одинаковых ссылки и при выборе не оригинальной, жертва сразу не поймет, так как они идентичны, однако при вводе логина и пароля, а затем и кода с карты кодов, жертва увидит ошибку и не сможет войти в «интернет-банкинг» своего банка. В это время мошенники, войдя в ее кабинет, похитят ее денежные средства.

К информации, поступающей из сети Интернет, связанной с деньгами, следует относиться достаточно серьезно. Схемы мошенничества разнообразны: это и просьбы о финансовой помощи, это и выигрыши в лотерее, звонки из банков, всевозможные дополнительные заработки и т.д.

**Данный перечень схем не является исчерпывающим, мошенники с течением времени придумывают все новые и новые схемы**

**КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ (ОБЯЗАТЕЛЬНО К ПРОЧТЕНИЮ):**

1) Никому и никогда не сообщайте подробную информацию о своей банковской карте. Пин-код, кодовое слово, CVV (или CVC2), код 3D-Secure и полученные от банка одноразовые пароли должен знать только владелец карточки.

2) Деньги стоит снимать и вносить только в проверенных банкоматах.

3) Если информация о карточке хранится в смартфоне или планшете, не следует читать сообщения, пришедшие с неизвестных номеров, и ни в коем случае не открывать ссылки в них.

4) Проверить свои социальные страницы на наличие конфиденциальной информации и возможность доступа к ней. «Привязать» страницу социальной сети к номеру мобильного телефона, а не к адресу электронной почты, помимо этого в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа».

5) При использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно, вы зашли на поддельную его копию.

6) Вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов.

7) Не используйте одинаковые логины и пароли на различных сайтах, слишком легкие пароли, либо те, о которых можно легко догадаться.

8) Остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях.

9) С осторожностью относитесь к письмам, в которых запрашиваются данные счетов, никогда не отправляйте финансовую информацию по незащищенным Интернет-каналам.

10) При поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, «VIBER», «TELEGRAM», «VK», «Одноклассники», «INSTAGRAM»), либо, в крайнем случае, идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам.

**Помните, что Вы можете оказаться в подобной ситуации в любой момент!**