Преступления в киберпространстве

В современном мире мало кто может представить свою жизнь без использования глобальной компьютерной сети Интернет. В настоящее время в сети Интернет совершаются следующие виды преступлений: хищение денежных средств с банковских платежных карт, распространение детской порнографии, вредоносных программных обеспечений, мошеннические действия при покупке вещей и иных товаров, а так же иные противоправные действия в отношении граждан, которые получили название-«киберпреступления». Появление новых социальных сетей, мессенджеров, гаджетов с использованием которых осуществляется выход в сеть Интернет, различных интернет-магазинов создают предпосылки для совершения преступлений в сети Интернет.

Из года в год количество «киберпреступлений» значительно увеличивается. Так в 2017 году по линии работы в сфере высоких технологий на территории Горецкого района было зарегистрировано 6 преступлений, в 2018 году- 22 преступления, а в 2019 году-43 преступления. Наиболее распространенными из них являются хищения денежных средств с банковских платежных карт (ответственность предусмотрена статьей 212 Уголовного кодекса Республики Беларусь-хищение путем использования компьютерной техники) и несанкционированный доступ к компьютерной информации (ответственность предусмотрена статьей 349 Уголовного кодекса Республики Беларусь). Рассмотрим наиболее частые примеры совершения вышеуказанных преступлений, имевших место в 2019 году:

Так гражданин А. утерял банковскую платежную карту, которой можно рассчитываться без введения пароля на сумму до 20 рублей Национального банка Республики Беларусь. Гражданин А. посчитав, что ее найдут и вернут ему либо же в отделение банка не блокировал утерянную им карту. Гражданин Б., нашедший вышеуказанную карту с ее использованием совершает различные покупки, в том числе и в интернет-магазинах, пока не потратит все денежные средства, находящиеся на текущем счету данной карты, после чего избавляется от найденной им банковской карты, выбросив ее в мусорную урну.

Злоумышленник, осуществив несанкционированный доступ к аккаунту гражданина Б. в социальной сети «Одноклассники» рассылает сообщения пользователям данной социальной сети, находящими в разделе «Друзья» у гражданина Б. Гражданин А. осуществляет вход на аккаунт в вышеуказанной социальной сети. В разделе «Сообщения» гражданин А. обнаруживает сообщение от гражданина Б. следующего содержания: «Привет», «В честь юбилея банк дарит всем его клиентам денежные средства в размере 150 рублей». «Я уже получил, хочешь и тебя научу?». Гражданин А. не задумываясь о том, что ведет переписку

не с гражданином Б., а с злоумышленником выступающем от имени гражданина Б. предоставляет по его просьбе последнему реквизиты своей банковской карты, а так же смс-код о регистрации в приложении «Интернет-банкинг» и пароль для входа в него. Злоумышленник, имея доступ к текущему (расчетному) счету гражданина А. совершает хищение денежных средств с его банковской карты путем переводы на свою (зачастую перевод осуществляется на счета зарубежных банков), в результате чего гражданину А. причинен имущественный ущерб на сумму, находящуюся на его банковской карте.

Исходя из способов совершения преступлений с банковских платежных карт граждан были выработаны правила, соблюдая которые вы не станете жертвой киберпреступника:

1. **Никому не передавайте свои банковские платежные карты**- при оплате картой в магазинах и иных торговых объектах не допускайте, что бы ваша карта пропадала из вашего поле зрения, даже на незначительное время, так как даже 15 секунд достаточно, что бы сфотографировать вашу карту с двух сторон и последующем совершить хищение денежных средств.
2. **Никому не сообщайте пин-код от своей банковской платежной карты**, так как лицо, знающее пароль от вашей карты может неправомерно ею завладеть, после чего совершить с ее использованием хищение денежных средств.
3. **Не записывайте пин-код банковской карты на самой карте,** так как при ее утере у лица, нашедшего вашу карту, появляется возможность совершить с нее хищение денежных средств**. Пин-код карты держите у себя в голове либо записывайте в телефоне, при этом нужно ограничить к нему доступ посторонних лиц.**
4. **Никому не сообщайте реквизиты вашей банковской платежной карты (номер, срок действия, секретный код),** так как в этом случае у лица появляется возможность совершить хищение денежных средств с вашей карты.
5. **Никому не сообщайте свой личный номер паспорта,** так как заполучив его злоумышленник сможет произвести регистрацию в «Интренет-банкинге» и совершить в дальнейшем хищение денежных средств с данного карт-счета.

Особое внимание следует уделить поведению граждан, попавших в следующую ситуацию: если же вам на мобильный телефон позвонило незнакомое лицо и представилось работником банка или же в социальных сетях пришло сообщение о том, что банк дарит денежные средства «просто так»- не при каких обстоятельствах не сообщайте

данным лицам реквизиты своих банковских карт, свои личные данные, код о регистрации в «Интернет-банкинге» и доступе в него.

Запомните- никогда работники банков не будут звонить вам и уточнять вышеуказанные сведенья, особенно в таких мессенджерах как Viber, WhatsApp и других.

Надеюсь, что данная статья поможет вам не стать жертвой злоумышленников, в том числе в глобальной компьютерной сети «Интернет».

Старший оперуполномоченный группы
раскрытия преступлений в сфере высоких
технологий криминальной милиции
Горецкого РОВД Александр Васильев