«Актуальные способы совершения преступлений, предусмотренных ст.208 УК Республики Беларусь, совершенные с использованием информационно-коммуникационных технологий»

Все преступления, предусмотренные ст. 208 УК Республики Беларусь, совершенные с использованием ИКТ, разделяются на две основные категории:

1. Вымогательства, совершенные с блокированием, модификацией или уничтожением компьютерной информации.

При этом в подавляющем большинстве случаев отмечается блокирование учетных записей «Apple iCloud» посредством ввода авторизационных данных (логин и пароль), предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

Способы предлогов довольно разнообразны:

Способ №1. Онлайн-знакомство жертвы с злоумышленником, представляющимся лицом противоположного пола.

Знакомство чаще всего происходит на тематических сайтах. Затем общение переходит в мессенджер, где новый знакомый под различными предлогами (например, необходимо срочно скачать какие-либо файлы или фото из облачного хранилища iCloud) вынуждает потерпевшего зайти в чужую учетную запись «Apple iCloud» со своего устройства. Для большего убеждения, злоумышленник использует заранее заготовленные фотографии, голосовые сообщения и видеозаписи, таким образом у жертвы складывается впечатление, что он действительно общается с лицом противоположного пола. Получив согласие, мошенник высылает логин и пароль, а после входа потерпевшим в «учетку» меняет пароль на iPhone и включает режим пропажи.

Способ №2. Реклама бесплатных игр и приложений в социальных сетях.

Злоумышленники осуществляют размещение видеозаписи (рекламы), в которой указывается бесплатный способ скачать ту или иную игру либо приложение, получить на свой баланс игровую валюту. Для установки данных предложений злоумышленники предлагают зайти в предоставленный ими аккаунт «Apple iCloud». Потерпевшими в подавляющем количестве случаев являются несовершеннолетние.

Способ №3. Трудоустройство.

Злоумышленники осуществляют размещение рекламы в сети-Интернет, в которой осуществляется поиск сотрудника на вакансию, как правило связанную с тестированием мобильных приложений для устройства «Apple», для чего предоставляют соискателю для входа якобы корпоративный аккаунт «Apple». В момент, когда жертва осуществляет вход в «Apple iCloud» она оказывается в ловушке, т.к. не может выйти из чужого аккаунта или отключить режим пропажи, iPhone остается заблокированным и не пригодным к использованию. И тогда злоумышленники предлагают перевести деньги за разблокировку устройства.

Запомните! Никогда не вводите логин и пароль чужие «учетки» на своих устройствах, а также не сообщайте никому свои учетные данные от аккаунта «Apple iCloud». Не переходите по неизвестным ссылкам и не вводите данные «Apple ID» на посторонних сайтах.

Совет родителям, чьи дети используют мобильные устройства «Apple»: мошенники не просто выманивают пароли, они стали добиваться того, чтобы ребенок сам, добровольно выполнил на своем iPhone вход в чужой iCloud. После этого устройство блокируется злоумышленником, и требуется выкуп. Как это происходит? «Бесплатные игры и приложения» рекламируют доступ к играм («PUBG Mobile», «Standoff2») и приложения («AioGram») в TikTok или Telegram. Ребенку в соцсетях или игровом чате новый «друг» предлагает установить мод, получить бонусы или «прокачать» персонажа. Для этого нужно «временно войти в его геймерский Apple ID» на своем устройстве. «Конкурс» или «Раздача призов», чтобы «получить приз», нужно подтвердить личность, войдя в предоставленный iCloud на своем устройстве. Мошенник утверждает, что это «временная процедура для проверки». Объяснение ребенку: «Призы не требуют входа в чужие аккаунты. Это 100% обман». Что происходит после входа в чужой iCloud? Активируется функция «Найти». Как только в Настройках → [Имя] появляется чужой Apple ID, мошенник со своего устройства сразу видит iPhone ребенка в списке своих. Устройство мгновенно блокируется. Мошенник дистанционно активирует «Режим пропажи» на iPhone. На экране появляется сообщение, что устройство утеряно и заблокировано. Появляется требование выкупа. Приходит сообщение с контактом мошенника и требованием заплатить за разблокировку.

Важно! Если ваш аккаунт заблокирован, разблокировка возможно только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

2. Вымогательства с угрозой распространения личной информации потерпевших либо иных сведений, которые последние желали сохранить в тайне.

К таким сведениям преимущественно относятся – фотографии и видеозаписи интимного характера, а также иные личные сведения, которые в большинстве случаев потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером для знакомства противоположного пола. В дальнейшем злоумышленник под предлогом распространения данных, среди круга знакомого жертвы, требует денежные средства.

Запомните! Не предоставляйте неизвестным лицам свои данные, содержащиеся в СМС-сообщениях и личные данные неизвестным лицам.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, все больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщать кому-то свои персональные данные. Ваша безопасность в первую очередь в Ваших руках.