Следственный комитет Республики Беларусь обращает внимание на появление и распространение нового способа мошенничества в сети Интернет

Анализ криминогенной обстановки и практики деятельности следственных подразделений свидетельствует о появлении и распространении на территории республики нового способа мошенничества.

Механизм его совершения заключается в подмене банковских реквизитов зарубежных контрагентов (Италия, КНР, Польша, ЮАР и иные) при осуществлении оплаты за поставку товаров.

Так, после согласования существенных условий контракта с зарубежным партнером, а в отдельных случаях и его подписания на электронную почту организации (предприятия) злоумышленниками направляется сообщение якобы от имени сотрудника иностранного контрагента об изменении реквизитов обслуживающего банка и необходимости перечисления денежных средств на новый счет (например, по причине уплаты значительного налога в прошлом банке, превышения лимита на счету, проведения в отношении предприятия государственного аудита).

При этом адрес электронной почты мошенников имеет существенное сходство с реальным, что зачастую остается незамеченным (например, e***@chainlon-com.pw вместо e***@chainlon.com.tw). Последующая переписка уже осуществляется с киберпреступниками.

Реализация подобной схемы хищения возможна посредством получения несанкционированного доступа к электронной почте одной из сторон сделки. В этой связи злоумышленники обладают информацией о предмете, условиях договора и могут вести переписку, не вызывая подозрения (в случае необходимости ими направляются дополнительное соглашение, счет-проформа (инвойс) с измененными реквизитами банковского счета и контактными данными представителей фирмы путем их «наложения» на подготовленные ранее и сохраненные в сообщениях документы). При этом письма реального контрагента автоматически переадресовываются в папку «Спам».

Кроме того, имеются обратные случаи, когда от имени белорусских субъектов хозяйствования путем компрометации их корпоративной почты в адрес зарубежных партнеров также направлялись письма, счета-проформы с измененными банковскими реквизитами. В результате денежные средства, причитающиеся белорусским предприятиям за произведенную (поставленную) продукцию, переводились на счета мошенников.

Необходимо отметить, что в рамках расследования указанной категории уголовных дел установлены факты использования сотрудниками субъектов хозяйствования корпоративной почты на домашних компьютерах, при регистрации в социальных сетях, личной электронной почты в служебных целях, а также пренебрежения минимальными требованиями к ее защите (отсутствие резервного адреса электронной почты, привязки к номеру мобильного телефона, установление пароля, который может быть подобран специальным программным

обеспечением в течение одной секунды). В ряде организаций доступ к электронной почте имело значительное число работников, не связанных с процедурой закупки товарно-материальных ценностей, его использование осуществлялось одновременно с нескольких компьютеров, а для входа не требовалось введения пароля (автоматическое сохранение в браузере).

В качестве мер, направленных на предупреждение указанных мошеннических действий, могут рассматриваться следующие:

исключение в деятельности организаций использования бесплатных почтовых сервисов, а также принятие дополнительных мер защиты корпоративной электронной почты (подключение двухфакторной аутентификации, соблюдение требований к сложности пароля и периодичности его смены, антивирусное программное обеспечение);

постоянный мониторинг корпоративной электронной почты администратором на предмет несанкционированного доступа (проверка истории входов в аккаунт, IP-адресов доступов, настроек переадресации);

ограничение и контроль доступа к компьютеру и электронной почте, используемым при ведении деловой переписки с зарубежными контрагентами;

проверка правильности адреса электронной почты контрагента при получении и отправке сообщений, а также поддержание контакта с его представителем и согласование ключевых вопросов дополнительно посредством иных средств связи (телефонных переговоров, использования факсимильной связи, мессенджеров);

проведение обучающих занятий с сотрудниками по безопасной работе в сети интернет и использованию электронной почты.

Source URL:
https://www.mpt.gov.by/sledstvennyy-komitet-respubliki-belarus-obrashchaet-vnimanie-na-poyavlenie-i-rasprostranenie-novogo