Букшта Н. Г.

ФИШИНГ КАК СПОСОБ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Букшта Назар Геннадьевич, курсант факультета милиции Академии Министерства внутренних дел Республики Беларусь, nbukshta@mail.ru

Научный руководитель – канд. юрид. наук Шинкевич А. М.

Проблема мошенничества стремительно перешла в интернет, который является необходимым инструментом современного общества. Это не только место поиска информации и общения, но также и комфортная среда для совершения различных преступлений, что можно рассматривать как глобальную проблему. Из всех преступлений, совершаемых в интернете, наибольшее распространение получили корыстные посягательства, связанные с обманом – мошенничество. Использование различного как прикладного, так и общедоступного программного обеспечения способствует обману жертвы и последующее завладение ее имуществом.

В настоящее время существует большое количество способов совершения интернет-мошенничества. Под способом совершения мошенничества в сети Интернет понимаются действия лица, посредством которых оно реализует свой преступный умысел, направленный на завладение чужими денежными средствами или получение права на их использование и распоряжение ими по своему усмотрению. Актуальными для Республики Беларусь способами совершения указанного вида преступления является фишинг и набирающий популярность в кругах киберпреступников – вишинг.

Фишинг, являясь одним из самых распространенных способов совершения интернет-мошенничества, представляет собой получение доступа к персональным данным пользователя (гражданина) для их дальнейшего использования в корыстных и преступных целях, полученных путем обмана или злоупотребления доверием, а также методов социальной инженерии (хакерства с использованием человеческого фактора) в сети Интернет.

В основном фишинг направлен на завладение реквизитами банковских карт, авторизационными данными доступа (логинами, паролями, идентификационными номерами паспортов, сеансовыми паролями и т. д.) к системе дистанционного банковского обслуживания, после получения которых совершается хищение денежных средств. Не всегда пострадавший самостоятельно заходит на сайт – «двойник», сайт может самостоятельно открываться в форме всплывающего окна.

Принцип работы фишинга состоит в перенаправлении пользователя на поддельные сетевые ресурсы, созданные злоумышленниками, внешне ничем не отличающиеся от подлинных интернет-страниц.

Переходя по прикрепленной к письму ссылке, пользователь попадает на поддельный сайт, который выглядит идентично подлинному сайту какого-либо банка или интернет-магазина, иными словами попадает на так называемый сайт «двойник». После того, как пользователь заполняет форму с логином и паролем, чтобы войти в свой аккаунт, он оказывается в распоряжении злоумышленников. Преступник, получая доступ к логину и паролю от аккаунта в интернет-банке, осуществляет перевод денежных средств со счета потерпевшего, тем самым совершая хищение.

Фишинговые ресурсы могут быть замаскированы под почтовые сервисы, торговые онлайн-площадки, игровые платформы и т. д., иными словами, интернет-ресурсы, тем или иным образом оказывающие финансовые услуги. Но, помимо этого, не теряет своей актуальности почтовый (с использованием рассылки электронных сообщений) и комбинированный фишинг.

Фишинговые сообщения, зачастую содержат информацию о сведениях, вызывающих тревогу (например, закрытие банковских счетов; обещаний большой денежной выгоды с минимальными затратами со стороны жертвы; сведениях о привлекательных сделках; запросах о пожертвованиях от лица благотворительных организаций). Ключевое отличие фишеров от хакеров в том, что они пользуются исключительно доверием граждан. Таким образом, они стремятся получить пароли, коды доступа, номера банковских карт и прочую конфиденциальную информацию, в зависимости от ситуации, разными путями.

Таким образом, распространение среди гражданского общества профилактических материалов по тематике фишинга, позволит совершенствовать навыки цифровой гигиены общества, а сотрудникам ОВД позволит эффективно противостоять вызовам в сфере киберпреступности.

Джумабаев Д. Дж.

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНВЕСТИЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Джумабаев Довлетбай Джумабаевич, магистрант Белорусского государственного университета, г. Минск, Беларусь,
dowletbayjumabayew@gmail.com

Научный руководитель: канд. юрид. наук, доцент Швед А. Н.

Проблемы уголовной ответственности за преступления в сфере инвестиционной деятельности представляются наиболее сложными как для ученых-юристов, так и для правоприменителей.

В соответствии со ст. 1 Закона Республики Беларусь от 12.07.2013 № 53-З «Об инвестициях» «инвестиции – любое имущество и иные объекты гражданских прав, принадлежащие инвестору на праве собственности, ином законном основании, позволяющем ему распоряжаться такими объектами,