УДК 343.985

Д.С. Якжик

О РОЛИ СЕРВИСОВ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ В ПРОТИВОДЕЙСТВИИ КИБЕРМОШЕННИЧЕСТВУ

Наиболее распространенным видом кибермошенничества является фишинг, и Беларусь не является исключением. Задача фишинга – «получить» конфиденциальные данные и использовать их, в том числе для получения доступа к денежным средствам пользователя. Выделяют две категории фишинга: обычный и целевой. Обычный фишинг (безадресный) отличается широким охватом и обычно имеет вид спам-кампаний. Целевой фишинг более технологичен. Злоумышленники собирают информацию о своих жертвах и впоследствии используют эти данные для составления убедительного и правдоподобного письма. Для достижения цели злоумышленнику необходимо привлечь внимание жертвы заголовком письма и добиться от нее выполнения ряда действий: открыть письмо, перейти по ссылке, ввести конфиденциальные данные в поля фишингового окна либо страницы. На каждом из этапов успех злоумышленника зависит от используемых уловок и приемов психологического манипулирования и от бдительности жертвы. По мере распространения фишинга накапливается статистическая информация о вероятности успешной атаки с использованием различных схем, при этом наиболее простые и успешные схемы ставятся на поток. Для начала преступной деятельности достаточно оплатить вступительный взнос и получить доступ к телеграм-чату с инструкциями, заготовками фишинговых ссылок и страниц, сетью наставников, технической поддержкой. Количество участников подобных чатов исчисляется сотнями.

Наиболее распространенной в настоящее время схемой мошенничества является «Мамонт» или «Курьер» – предложение о покупке товара по объявлению на электронной торговой площадке. Мошенник выбирает объявления, в которых указан номер мобильного телефона продавца и направляет в мессенджере сообщение о заинтересованности в покупке товара, при этом сообщает, что находится в другом регионе, предлагает оплатить товар переводом с карточки на карточку и воспользоваться службой доставки. Жертва, движимая желанием продать товар, соглашается принять оплату на свою банковскую платежную карточку, после чего ей направляется поддельный запрос от банка на зачисление денежных средств, в котором требуется указать реквизиты карточки и CVV/CVC код (VISA использует обозначение CVV (Card Verification Value), MasterCard использует обозначение CVC (Card Validation Code)). Цель мошенников – использовать полученные реквизиты для покупки криптовалюты, но им не хватает сеансового ключа 3D Secure, поступающего по SMS на телефон держателя карточки. Поэтому продавцу направляется окно для ввода кода, якобы для зачисления платежа на карточку. В результате мошенники получают все необходимое для однократного использования карточки жертвы в своих целях, процесс может развиваться далее для получения новых сеансовых ключей и данных других банковских карточек.

Залогом успеха описанной схемы является наличие в объявлении на торговой площадке необходимой мошеннику на первоначальном этапе информации: номер мобильного телефона жертвы и психологический триггер – желание продать определенную вещь.

Социальная инженерия в подобных схемах базируется на двух факторах. Во-первых, осведомленность держателя карточки о конфиденциальной информации, необходимой для дистанционного списания средств со счета. Во-вторых, отсутствие у продавца опыта совершения сделок с получением платежа на банковскую платежную карточку, что создает неуверенность в себе и повышает восприимчивость к манипулированию со стороны «искушенного покупателя». Незнание того, что для зачисления средств достаточно сообщить отправителю только номер карточки (для некоторых банков эмитентов дополнительно потребуется либо срок действия карточки либо имя и фамилия владельца). В любом случае отправителю не требуются CVV/CVC код карточки получателя, а при зачислении средств на карточку не генерируется ключ 3D Secure.

Условием успешной защиты от уловок мошенников является исключение любого из указанных факторов. В целях снижения восприимчивости граждан к методам социальной инженерии в последние годы в Беларуси ведется широкомасштабная информационная кампания по разъяснению населению способов защиты от фишинга и вишинга. К сожалению, практика показывает, что осведомленность людей не гарантирует защиту от мошенников.

Вместе с тем первый фактор – осведомленность держателя карточки о конфиденциальных сведениях, открывает доступ к широкому спектру мер противодействия кибермошенничеству. Возможно ли пользоваться банковской платежной карточкой без данных о держателе, номере карточки, сроке действия, CVV/CVC коде? Да, и многие делают это ежедневно, когда прикладывают карточку к картридеру, оплачивая товары либо услуги.

Традиционная технология приложений на базе смарт-карт состоит в двухступенчатой аутентификации. Сначала владелец смарт-карты локально аутентифицируется относительно смарт-карты при помощи пин-кода через кардридер, а затем смарт-карта исполняет более слож-

ный криптографический протокол аутентификации, включающий, например, вычисление цифровой подписи. В процессе аутентификации используются протоколы с защитой данных.

В настоящее время в торговле набирает популярность мобильный SoftPOS-эквайринг. Он дает возможность принимать безналичные платежи с помощью смартфона с NFC-модулем (Near Field Communication). Для покупателя процесс оплаты выглядит аналогично покупке при помощи обычного платежного терминала. Он прикладывает свою бесконтактную карточку к смартфону продавца, на котором установлено приложение SoftPOS-эквайринга. После обработки платежа у продавца на экране телефона отображается информация об успешно проведенной операции, а покупатель получает оплаченный товар или услугу. Электронный чек приходит в виде SMS.

Адаптация функционала SoftPOS-эквайринга к переводам с карточки на карточку (P2P-переводам) позволит продавцу выставлять электронный счет, а покупателю акцептовать его, приложив свою карточку к смартфону.

Для дистанционных сделок возможным решением является интернет-эквайринг. В процессе оформления приобретаемого товара или услуги покупатель покидает сайт продавца и перенаправляется на специальный защищенный сайт банка-эквайера, что можно сразу заметить в адресной строке браузера. При оплате покупок в интернете вместо терминала используется специальный защищенный сервис банка.

Организация платежного сервиса на электронных торговых площадках имеет ряд положительных факторов и для торговой площадки, и для продавцов, и для покупателей. Средства покупателя депонируются на счете торговой площадки до получения от покупателя подтверждения о соответствии товара заявленному в объявлении о продаже, после чего перечисляются продавцу. На счетах торговой площадки формируется оборотный капитал, что создает источник средств для инвестирования и дополнительного дохода. Продавец сообщает сведения о своей банковской платежной карточке только торговой площадке, что защищает его от социальной инженерии мошенников на стороне покупателя. Покупатель приобретает дополнительную защиту своих прав. В случае получения товара ненадлежащего качества он имеет возможность расторгнуть сделку, вернуть товар продавцу и вернуть удерживаемую торговой площадкой уплаченную сумму.

Менее технологичным и менее защищенным вариантом является информационное взаимодействие электронной торговой площадки с банковскими сервисами переводов с карточки на карточку (P2P-переводы). Идея заключается в создании возможности сторонам сделки перейти с сайта торговой площадки на страницу банка эмитента

карточки покупателя с официальной информацией об условиях перевода с карточки на карточку.

Таким образом, дальнейшее развитие используемых и создание новых сервисов безналичной оплаты товаров и услуг для физических лиц позволит отказаться от использования CVV/CVC кодов и создать механизм противодействия кибермошенничеству с применением социальной инженерии.

УДК 340.1

К.В. Янчуревич

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КАК ВАЖНЫЙ ЭЛЕМЕНТ ПРОЦЕССА ФОРМИРОВАНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РЕСПУБЛИКЕ БЕЛАРУСЬ

В настоящее время в ряде стран наблюдается процесс активного формирования и развития информационного общества. В зависимости от множества различных факторов отдельные государства находятся на разных этапах вышеуказанного процесса.

Следует отметить, что информационное общество представляет собой сложную систему, которая включает в себя множество элементов. Большинство ученых, занимавшихся исследованиями в области информационного общества, сходятся во мнении, что именно информация, по сути, и является центральным звеном («ядром») информационного общества.

Необходимо подчеркнуть, что для того чтобы общество могло беспрепятственно пользоваться информацией, распространять ее, а также ощущать защищенность от преступных посягательств со стороны преступников, следует применять высокоэффективные действенные меры.

Безусловно, уже разработано и активно применяется на практике достаточно много способов борьбы с киберпреступлениями (правовые, организационно-технические и др.). Вместе с тем факт наличия значительного количества киберправонарушений свидетельствует о необходимости разработки и использовании на практике новых эффективных способов борьбы с данными правонарушениями.

Считаем целесообразным, наряду с уже используемыми методами обеспечения кибербезопасности, применение следующих:

1. Включение в образовательный процесс учащихся школ и средних специальных учебных заведений, а также учреждений высшего образо-