# КАК НЕ СТАТЬ ЖЕРТВОЙ В КИБЕРПРОСТРАНСТВЕ

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники. В Республике Беларусь отмечается ежегодный рост преступлений, связанных с хищением денежных средств организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Подавляющее большинство данных преступлений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании слабостей человеческого фактора и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров, за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами. То же самое касается и банковских карт: преступниками совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организаций и т.д.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные 1Т-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

Происходит совершенствование форм и методов, используемых преступниками в сфере высоких технологий, применение ими новейших информационных технологий, использование уязвимостей современных информационных коммуникаций, в связи с этим количество выявленных преступлений увеличивается.

Анализ состояния оперативной обстановки на территории Толочинского района в сфере высоких технологий за 2020 год в сравнении прошлым годом свидетельствует о значительном росте (с 13 до 37) количества зарегистрированных преступлений по линии СВТ. Несмотря на рост преступлений, удельный вес установления подозреваемых от зарегистрированных преступлений по линии СВТ на территории района составил 13,5%. Как правило данные преступления совершаются из-за пределов Республики Беларусь и установление лиц, их совершивших, представляет определённую сложность.

Преступность в сети Интернет приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег, практически полная безнаказанность, анонимность преступников, большое количество доверчивых людей – все это подпитывает этот своеобразный «бизнес».

**Виды корыстных преступлений в сети Интернет**

Простые пользователи сети Интернет могут стать жертвами следующих преступных посягательств, совершаемых по корыстным мотивам:

**Кардинг** – вид преступления, представляющий способ мошенничества с банковскими картами. Мошенниками производится похищение реквизитов банковских карт с помощью взлома серверов интернет-магазинов, систем платежей, с персонального компьютера пользователя или иным доступным им путем.

Разновидностью кардинга является **фишинг**. Это уведомления, отправленные якобы администраторами систем платежей, от имени банка, почтовых серверов или из соцсетей. В этих уведомлениях содержатся призывы пройти по указанной ссылке, чтобы украсть учетные данные пользователя. Целью таких манипуляций может быть счет в банке, учетная запись в платежных системах, электронная почта и социальные сети.

**Уведомления о выигрыше**. Этот вид преступления заключается в том, что пользователю присылается сообщение о том, что он будто бы получил приз в виде крупной суммы денег или автомобиля. Затем мошенники пытаются выманить у пользователя определенную сумму денежных средств будто бы для получения его выигрыша (налог, страховка, банковские услуги и т.д.).

**Нигерийский спам**. Довольно старая схема мошенничества, известная еще до распространения сети Интернет. Первоначально нигерийские письма рассылались по обычной почте. Пользователь получает письмо, где автор письма заявляет, что у него есть миллионы долларов, которые нужно вывести за рубеж. Автор просит пользователя помочь ему в обналичивании крупной суммы денежных средств, обещая за услугу несколько процентов от этой суммы.

**Попрошайничество в интернете**. Пользователю доставляется сообщение с призывом о помощи от благотворительных организаций или людей, оказавшихся в беде. Такие письма содержат данные реальных фондов и людей, но реквизиты предоставляются мошенниками.

**Интернет-аукционы**. Продавцы выставляют товар на аукцион, но для повышения ставок используют ботов, либо повышают их сами, чтобы пользователь не смог купить выставленный товар подешевле.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперссылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

Чтобы не стать жертвой подобных преступлений, в первую очередь, кардинга – никому и никогда не сообщайте подробную информацию о своей банковской карте. Пин-код, кодовое слово, CVV (или CVC2), код 3D-Secure и полученные от банка одноразовые пароли должен знать только владелец карточки. Даже если звонит якобы представитель банка или владелец карточки получает SMS или сообщение по сети Интернет о блокировке карты, эти данные никому нельзя сообщать. Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, владельца карточки попросят приехать в банк лично.

Если часто происходит оплата заказов в онлайн-магазинах, можно создать виртуальную карточку и делать покупки только с ее помощью. Многие банки выпускают «виртуалку» бесплатно.

Деньги стоит снимать и вносить только в проверенных банкоматах. Лучше всего в отделениях банков и охраняемых торговых центрах.

Следует также подписаться на банковские sms-уведомления. Это позволит быть в курсе всех операций по карточке. Если этот вариант не нравится (сегодня такая опция чаще всего не бесплатна), можно ежедневно просматривать выписку в личном кабинете или приложении.

Если банк предлагает такую возможность, следует установить лимиты на операции, связанные с оплатой и переводами. Сделать это можно самостоятельно (в личном кабинете или приложении) или через колл-центр.

Также рекомендуется не входить в личный кабинет или приложение через общедоступный Wi-Fi.

Если информация о карточке хранится в смартфоне или планшете, не следует читать сообщения, пришедшие с неизвестных номеров, и ни в коем случае не открывать ссылки в них.

**Основные правила информационной безопасности по защите банковской карточки**:

хранить в тайне пин-код карты;

прикрывать ладонью клавиатуру при вводе пин-кода;

оформлять отдельную карту для онлайн-покупок;

деньги зачислять только в размере предполагаемой покупки;

использовать услугу 3-D Secure и лимиты на максимальные суммы онлайн-операций;

скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его.

**Не рекомендуется**:

хранить пин-код вместе с карточной (на карточке);

сообщать CVV-код или отправлять его фото;

распространять личные данные (например паспортные), логин и пароль доступа к системе «Интернет-банкинг»;

сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароли 3-D Secure.

**Как не стать жертвой преступлений**

**против информационной безопасности**

Основным источником опасности для пользователей компьютеров были и остаются вредоносные программы, которые с развитием сетевых технологий получили новую среду для своего распространения.

Вредоносные программы можно разделить на три группы:

- компьютерные вирусы;

- сетевые черви;

- троянские программы.

Одной из разновидности вирусов является блокировщик Windows. Вирус проникает на компьютер пользователя (этот процесс может происходить автоматически и незаметно) и добавляет свой код в автозапуск системы. После перезагрузки компьютера операционная система блокируется, появляется сообщение о необходимости оплатить некоторую сумму денег на указанный счет или отправить смс на номер телефона. При этом могут содержаться угрозы об уничтожении данных.

Чтобы не стать жертвой преступлений против информационной безопасности, следует неукоснительно следовать рекомендациям технических специалистов. Компьютеры и используемые ими операционные системы могут предназначаться для различных целей и использоваться в различных условиях. Поэтому общих, единых для всех случаев рекомендаций не существует. Так, например, использование программного обеспечения для противодействия вирусной угрозе («Антивирус») на компьютере, подключенном к сети Интернет, будет иметь эффект, а на компьютере, подключенном к ведомственной сети передачи данных, эффект будет иметь только тот Антивирус, который требуют установить технические специалисты.

**Как не стать жертвой преступлений в социальных сетях**

Социальные сети, форумы, блоги – это среда с практически мгновенной скоростью распространения информации и довольно сильным эффектом памяти (содержимое многих социальных ресурсов индексируется и доступно из поисковиков). Кроме того, растет индекс доверия к этим источникам информации.

Сегодня в социальных сетях наблюдается целый спектр различных угроз, включая вредоносный код и спам. Кроме того, это поле деятельности для применения методов социальной инженерии на базе фишинга: злоумышленники могут использовать их как для распространения злонамеренного кода, так и для разведки, чтобы затем осуществить направленную атаку.

Более того, использование социальных сетей повышает риск утечки: невнимательный, недисциплинированный или нелояльный сотрудник может опубликовать там информацию ограниченного доступа. Ситуация усугубляется тем, что в социальных сетях потенциальные злоумышленники могут неформально общаться с сотрудниками на любые темы, следовательно, появляется гораздо больше возможностей для социальной инженерии и получения с ее помощью конфиденциальной информации.

Основная проблема социальных сетей – это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг компании, бренда или человека. Но с другой стороны, это открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив – он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

Вторая угроза – это так называемый маскарад, или возможность подмены личности: доподлинно неясно, кто именно скрывает свои действия под именем друзей или прикрывается фотографиями знакомых в профиле социальной сети. Если при переписке по электронной почте можно было бы по IP-адресу отправителя собрать о нем хотя бы какую-то информацию, то в социальных сетях это не получится. Сценарий подобного маскарада возможен и на ведомственном уровне.

Третья угроза связана со взломом пользовательских записей социальных ресурсов. Посредством взлома злоумышленник может проникнуть в социальную сеть (в том числе от имени того, кто представляет в ней ведомство), разослать по ее списку друзей фишинговое (или заведомо ложные) сообщение и получить деньги либо мотивировать получателей к каким-либо негативным действиям – в частности, пройти по указанной ссылке и запустить вредоносный код.

Первый заместитель отдела внутренних дел

Толочинского райисполкома В.В.Микульчик