ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ

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.

Так называемый **фишинг** – тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия используется также для распространения троянских коней: эксплуатируется любопытство, либо алчность объекта атаки. Злоумышленник направляет e-*mail, sms-сообщение или сообщение в мессенджере,* во вложении которого содержится, например, важное обновление антивируса.

Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперсылкам. 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.

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 организации и т.д.

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

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

Основные виды мошенничества с банковскими картами

Скимминг

Мошенники устанавливают на банкомат специальное устройство, считывающее данные банковской карты

Телефонное мошенничество

Звонки и смс-сообщения под разными предлогами, чтобы выманить банковские реквизиты или деньги у жертвы

Хищение данных с помощью вирусов

Рассылка на устройства потенциальных жертв вредоносного ПО

Фишинг

Создание поддельного сайта, имитирующего подлинный, для получения доступа к данным пользователя (логины, пароли и др.)

Мошенничество при покупках в интернете

Мошенник представляется покупателем и, под предлогом перевода денег, узнает реквизиты карты

ПРАВИЛА, КОТОРЫЕ ПОМОГУТ ВАМ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЙ:

- храните номер карточки и ПИН-коды в тайне;
- не используйте один пароль для всех интернет-ресурсов;
- к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;
- регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;
- поставьте лимит на сумму списаний или перевода в личном кабинете банка;
- не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;
- не переводите денежные средства на счета незнакомых лиц;
- не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;
- будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно;
- не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;
- не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
- насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;
- не размещайте в открытом доступе и не передавайте информацию личного характера.

Особое внимание следует уделить вопросам безопасности детей, которые могут стать жертвой преступлений, совершаемых с использованием компьютерных технологий и сети Интернет. Это может быть как банальное вымогательство, так и совершение преступлений сексуального характера, склонение к суицидальному поведению. Помните, доверительные отношения с ребенком в большинстве случаев помогут предотвратить совершение в отношении него преступлений, в том числе в сети Интернет

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

- необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;
- никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.

ПРАВИЛА БЕЗОПАСНОСТИ, КОТОРЫЕ ДОЛЖНЫ ЗНАТЬ ВЫ И ВАШИ ДЕТИ:

- приучите детей посещать только те сайты, которые Вы разрешили;
- примите все меры, чтобы ребенок перед распространением своей личной информации советовался с Вами и предупреждал Вас об этом;
- запретите скачивать что-либо в сети Интернет без Вашего разрешения;
- помогите детям защититься от спама (массовой рассылки коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать);
- беседуйте с детьми о том, что нового они узнали из интернет-ресурсов, появились ли у них новые друзья в социальных сетях, какие темы они обсуждают;
- убедитесь в том, что ребенок советуется с Вами перед встречей с лицом, с которым он познакомился в сети Интернет, перед покупкой или продажей каких-либо вещей с использованием «глобальной паутины»;
- обсудите с ребенком возможные риски при участии в азартных играх;
- постоянно напоминайте несовершеннолетнему о негативных последствиях, к которым может привести разглашение его личной информации;
- контролируйте, какими чатами и сайтами пользуется ребенок. С этой целью установите на компьютерных устройствах программу, блокирующую посещение ребенком «опасных» сайтов; установите на своих мобильных устройствах приложения, предусматривающие уведомления родителей о посещении (или попытке посещения) ребенком «опасного» сайта;
- обращайте внимание на изменение поведения подростка (угнетенное настроение, повышенная тревожность, нежелание делиться с Вами информацией о том, с кем он общается, какие у него и его друзей общие интересы), что может являться признаком совершения противоправных деяний в отношении несовершеннолетнего, в том числе с использованием сети Интернет;
- объясните детям, что при поступлении оскорблений, незаконных требований и угроз в их адрес, им необходимо сразу же сообщить об этом взрослым, поскольку они всегда найдут поддержку и защиту в Вашем лице.

6 правил информационной безопасности

GROUP-IB

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам
+ Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

× Использовать повторения символов
× Хранить пароли на бумажных носителях
× Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
× Сохранять пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
+ Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

× Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

6 правил информационной безопасности

GROUP-IB

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники

× Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
+ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

× Размещать персональную и контактную информацию о себе в открытом доступе

× Использовать указание геолокации на фото в постах

× Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса

× Употреблять ненормативную лексику при общении

× Устанавливать приложения с низким рейтингом и отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ Хранить в тайне пин-код карты
+ Прикрывать ладонью клавиатуру при вводе пин-кода
+ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
+ 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

× Хранить пин-код вместе с карточкой / на карточке

× Сообщать CVV-код или отправлять его фото

× Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»

× Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.