МАТЕРИАЛ
для членов информационно-пропагандистских групп
(октябрь 2023 г.)

«Профилактика киберперступности и преступлений, совершенных с использованием информационно-коммуникационных технологий»

Материал подготовлен
Управлением по противодействию киберпреступности
криминальной милиции УВД Гродненского облисполкома

Повсеместное внедрение и использование компьютерных информационных технологий, безусловно, создает возможности для более эффективного развития экономики, политики, общества и государства в целом. Однако совершенствование и применение высоких технологий приводит не только к укреплению информационного общества, но и появлению новых угроз, одной из которых является компьютерная преступность.

Рассмотрим основные угрозы, которым подвергаются пользователи в современном киберпространстве.

Вишинг – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

В большинстве случаев при совершении звонков потерпевшим преступники используют IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную

оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

Фи́шинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т. д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

Стоит отметить, что применяемая злоумышленниками схема хищений характерна не только для Беларуси. Столь же системно эти преступления совершаются в отношении пользователей схожих ресурсов, ориентированных на иные государства СНГ: России (avito.ru), Украины (olx.ua), Казахстана (olx.kz) и др.

Сватинг – заведомо ложный вызов полиции, аварийно-спасательных служб, путем фальшивых ложных сообщений об опасности (например, о минировании, убийствах, захвате заложников).

Сватинг в первую очередь распространен в среде, где люди, чаще всего молодые, объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о минировании какого-либо объекта.

В последние годы сватинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Общественная

опасность таких деяний состоит в том, что заведомо недостоверные сведения дезорганизуют нормальную работу объектов транспорта, предприятий, государственных органов и учреждений, организаций независимо от формы собственности. В свою очередь, это причиняет существенный экономический вред как субъектам хозяйствования, так и гражданам. При этом информация о возможном взрыве, поджоге либо иных действиях, предполагающих тяжкие последствия, способна посеять панику среди населения и внести неудобства в повседневную жизнь.

Стоит отметить, что ответственность за это преступление наступает с 14 лет. Наказание – штраф, арест, ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет. Если ребенку, сообщившему о ложном минировании, не исполнилось 14 лет, наступает административная ответственность родителей, а ребенка ставят на учет в инспекцию по делам несовершеннолетних.

DoS – это атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен. В настоящее время DoS и DDoS-атаки популярны тем, что позволяют довести до отказа практически любую систему.

Обычно атака организуется при помощи троянских программ. Предварительно трояны заражают недостаточно защищенные компьютеры обычных пользователей и могут довольно долгое время никак себя не проявлять на зараженном компьютере, ожидая команды от своего хозяина. Компьютер может подвергнуться такой атаке при посещении различных зараженных сайтов, при получении электронной почты или при установке нелицензионного программного обеспечения. Когда злоумышленник собирается начать атаку, он дает команду, и все ранее зараженные компьютеры начинают одновременно слать запросы на сайт-жертву.

Наиболее массовая DoS-атака в Беларуси была произведена экстремистскими каналами в 2021 году. Злоумышленники, намеренно утаивая информацию об уголовной ответственности за участие в DoS-атаке, привлекли к участию в ней более 10 тысяч граждан (преимущественно из числа молодежи). Практически все участники этого противоправного действия были установлены, а наиболее активные из них были привлечены к уголовной ответственности.

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить

ребенка прислать фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

От груминга отличают секстинг — это пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.

Порой под влиянием ситуации или эмоций, может показаться, что переслать такие фото – хорошая идея. Чаще всего парни и девушки делают это флиртуя, поддавшись настойчивым уговорам, пытаясь развлечь своих друзей, чтобы получить их признание (чаще пересылают чужие фото, чтобы похвастаться), или же просто отомстить. Эта идея, прямо скажем, не очень хорошая: злоумышленник может воспользоваться такой доверчивостью во вред.

Кибербуллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

Эта форма психологического террора может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве; физическая агрессия и так далее. Причины кибербуллинга: чувство превосходства, зависть, чувство превосходства над соперником, чувство собственной неполноценности, самореализация.

Особо следует отметить способ воздействия запрещенным контентом. Ребенку могут показывать порнографические материалы, нанося ущерб психике, так как изображенное со временем перестанет восприниматься ребенком как аморальное поведение.

Угроза нового времени – так называемые группы смерти. И хотя обычно создателями таких групп являются сами подростки (цель – «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

МОШЕННИЧЕСТВО В СОЦСЕТЯХ

В настоящее время особо актуальной становится проблема защиты аккаунтов в социальных сетях и противодействия различным формам и видам мошенничества. Наиболее типичные способы обмана в соцсетях сегодня таковы:

Предоплата

Злоумышленники размещают объявления о продаже каких-либо товаров по бросовым ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

Шантаж и вымогательство

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

Онлайн-игры

Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

Родственник совершил ДТП

В последнее время участились случаи телефонного мошенничества. Например: пожилому человеку звонит по телефону незнакомец и, представляясь сыном, дочерью, внуком, заявляет: «Я попал в ДТП! Мне срочно нужна помощь!». Если возникает вопрос, что с голосом, на другом конце провода отвечают, что «пострадавший» повредил губу, выбил зубы, называют другие причины, заговаривая жертву, не оставляют шансов на разумные действия. После чего «родственник» передает трубку якобы сотруднику правоохранительных органов, который ведет дальнейший разговор и выманивает деньги, давая понять, что ситуация критичная. Пожилой человек на эмоциях соглашается на все условия. После беседы по телефону к нему приезжает курьер и забирает деньги. Иногда мошенники

представляются сотрудниками милиции либо следователями. Говорят, что близкий родственник, сын или дочь, совершили аварию и сбили человека. И чтобы избежать ответственности, необходимо заплатить деньги. Если собеседник соглашается, он называет адрес, и вскоре к нему приходит человек и забирает деньги.

СОВЕТЫ ПО БЕЗОПАСНОСТИ

- никогда, никому и ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов;

- не следует сообщать в телефонных разговорах и при общении в соцсетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений;

- в случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты. Сообщите о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка не звонил;

- в случае поступления звонка «от попавшего в ДТП родственника» либо «сотрудника милиции» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить данному, либо иному родственнику либо иному другому лицу у которому можно перепроверить информацию. Далее, незамедлительно сообщить о данному факте в милицию и ни в коем случае не передавать никому денежных средств;

- в том случае, если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и банк это заметит, то его сотрудники сперва инициативно заблокируют банковскую платежную карту, затем сообщат Вам причину принятого решения (ничего не уточняя) и пригласят посетить банк с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам! Никогда не устанавливайте по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer» и др. Не сообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернет банкинга на Вашем устройстве и совершить хищение денежных средств. Учтите:

сотрудники банков никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»);

- в настоящее время просто необходимо наличие второй банковской платежной карты, не привязанной к основному банковскому счету (например, зарплатному). Этой картой рассчитывайтесь в сети Интернет, заранее пополняя ее на необходимую сумму. В таком случае Вы сможете обезопасить свой основной банковский счет. Многие банки предлагают своим клиентам услугу выпуска «виртуальной карты». Процесс ее открытия не требует посещения клиентом банка и представляет собой достаточно быстрый процесс. В итоге Вы станете обладателем электронного аналога банковской карты, посредством которой сможете рассчитываться за услуги в сети Интернет без риска скомпрометировать основной банковский счет. Просто перед оплатой пополните ее необходимой суммой с основной карты - и никаких проблем!;

- каждый владелец банковских платежных карт может настроить собственный алгоритм безопасности при их использовании. Для обеспечения сохранности денежных средств, размещенных на банковских счетах, каждый держатель карточки посредством систем дистанционного банковского обслуживания может установить индивидуальные ограничения (лимиты/запреты). Среди основных - следующие: подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов в сети Интернет); установление банком-эмитентом ограничение на проведение расходных операций (максимальная сумма и количество операций в определенный период времени); возможность самостоятельно устанавливать ограничения (на проведение операций в сети Интернет, на совершение операций в конкретной стране, на совершение отдельных видов операций);

- для доступа к системам дистанционного банковского обслуживания и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора. Рекомендуется составлять комбинации паролей не менее чем из 12 знаков (цифры, буквы и символы в разном регистре). Создавайте уникальные пароли для каждого сервиса в отдельности. Стоит воздержаться от паролей, составленных из дат рождения, имен, фамилий - то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей). Также следует регулярно менять пароли, чем чаще - тем лучше. Пользуйтесь только проверенным менеджерам паролей!;

- при поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек - не следует сразу же

отвечать на подобные сообщения! Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться с этим человеком (по телефону, лично встретиться) и уточнить, действительно ли он нуждается в помощи;

- в целях защиты устройств необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систем. Установить антивирусную программу следует не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.