УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ МИНСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

УТВЕРЖДАЮ
начальник управления
по противодействию киберпреступности
криминальной милиции
УВД Минского облисполкома
подполковник милиции

А.С.Грицук

04 .05.2023

ПЛАН-КОНСПЕКТ

«Об актуальных вопросах и условиях совершения посредством глобальной компьютерной сети Интернет и телефонии мошенничеств, а также иных киберпреступлений»

Минск 2023

ВВЕДЕНИЕ

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.

Экспоненциально увеличивающийся поток информации и преобладание цифровой информации в образовательной среде современной школы актуализируют проблему профилактики цифровой безопасности современных школьников. Особое место в данном вопросе принадлежит профилактике цифровой зависимости школьников, поскольку дети проводят в интернете довольно много времени.

Как известно, интернет не только содержит множество полезной информации и предоставляет выбор развлечений, но и таит массу угроз, которые могут повлиять и на материальное состояние семьи, и на психологическое здоровье детей.

На текущий момент возраст интернет-пользователя снизился настолько, что порой пятилетние малыши обращаются с компьютером и мобильными устройствами более ловко, чем взрослые. Помимо всех известных положительных моментов, интернет несет в себе опасность, которая может затронуть даже пользователей младшего дошкольного возраста.

Рассмотрим основные угрозы, которым подвергаются граждане в современном киберпространстве.

1. ВИШИНГ

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.

2. ФИШИНГ

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.

3. СВАТИНГ

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.

4. ДДОС-атаки

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.

5. КАРДИНГ

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.

Распространенным способом таких хищений является использование подлинной БПК, которая по какой-то причине выбыла из пользования законного владельца (украдена, утеряна, передана самостоятельно).

6. 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.

7. ТАКТИКА РАЗГОВОРА ЗЛОУМЫШЛЕННИКА С ПОТЕРПЕВШИМИ, СПОСОБЫ ИХ СКЛОНЕНИЯ К ПЕРЕДАЧЕ ДЕНЕЖНЫХ СРЕДСТВ (ПРИМЕРЫ).

Как указывалось ранее, злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков или правоохранителей, под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах системы двухфакторной аутентификации, а также склоняют к установлению на мобильный телефон приложений удаленного доступа.

Далее приведены типичные случаи совершения хищений денежных средств с карт-счетов жителей Минской области.

В правоохранительные органы с заявлением обратилась пенсионерка из г. Марьина Горка Пуховичского района, которая сообщила, что у нее с различных банковских счетов, в период времени с 1 февраля по 19 апреля 2023 года, в общей сумме похитили денежные средства в размере более 150 тысяч белорусских рублей.

Как пояснила потерпевшая, в начале феврале 2023 года ей позвонил неизвестный мужчина, который представился сотрудником милиции и сообщил, что ее карту пытаются взломать и снять с нее денежные средства. Для того, чтобы этого не произошло, ей необходимо установить приложение «RustDesk» и сообщить данные из смс-сообщений. Пенсионерка выполнила данные указания, а также в последующем сообщила о наличии у нее иных карт, на депозитах которых имелись вклады в Евро и в белорусских рублях, а также срок истечения данных депозитов. Злоумышленник посредством приложения для удаленного доступа «RustDesk» завладел реквизитами доступа

к личному кабинету потерпевшей, после чего получил доступ к карт-счету и завладел денежными средствами в общей сумме свыше 150 тысяч рублей.

В правоохранительные органы с заявлением обратился житель г. Несвижа, который сообщил, что у него, в период времени с 31 марта по 1 апреля 2023 года, мошенники похитили денежные средства в размере более 62 тысяч белорусских рублей.

Как пояснил потерпевший, в конце марта 2023 года ему позвонила неизвестная женщина, которая представилась сотрудником милиции и пояснила, что гражданин С. пытался взять кредит на его имя и спросила, оставлял ли он в последнее время где-либо свои данные. Указанные сведения потерпевший сообщил. После чего женщина уведомила, что переключит его для дальнейшего общения с сотрудником службы ассоциации банков – гражданином К. Вышеуказанный сотрудник сказал потерпевшему, что для того, чтобы обезопасить его счета от мошенников, необходимо установить приложения для удаленного доступа «RustDesk». Далее на потерпевшего была открыта цифровая карточка. Также в ходе телефонного разговора гражданин К. сообщил потерпевшему, что сотрудниками милиции проводится проверка по факту того, что на его имя пытались взять кредит, поэтому по месту жительства мужчины будет проведен обыск, в ходе которого будут изъяты все крупные суммы денег и вернут их не скоро. В связи с этим все наличные денежные средства, которые есть дома у потерпевшего необходимо зачислить на номер счета, который ему сообщат. В течение двух дней мужчина обменял все накопления на общую сумму 61 600 белорусских рублей, которые имелись в валюте, и зачислил на счет, указанный мошенниками. Также посредством приложения «RustDesk» с его счета было списано 1 100 белорусских рублей.

8. ТИПИЧНЫЕ КРЕДИТНЫЕ ПРОДУКТЫ, ПРЕДЛАГАЕМЫЕ ИЛИ ИСПОЛЬЗУЕМЫЕ ПРИ ПОЛУЧЕНИИ ДЕНЕЖНЫХ СРЕДСТВ.

Кибермошенники могут выдавать себя за кого угодно, например за представителя службы безопасности банка или сотрудника органов внутренних дел. Как правило, предлогом для звонка является обнаружение фактов несанкционированных денежных переводов с банковского счета за рубеж, которых на самом деле не было. Кроме того, часто используется мошенническая схема «оперативная игра». В ходе телефонной беседы в популярных мессенджерах жертве предлагается принять участие в оперативной игре по изобличению неблагонадежного сотрудника банка путем оформления кредита,

который зачисляется на банковский счет. При этом могут использоваться поддельные служебные удостоверения сотрудников органов внутренних дел. Приведенные выше мошеннические схемы направлены не иначе как на хищение денежных средств под благовидным предлогом.

Как Вы можете узнать, что Вас пытаются обмануть? Самый простой способ – это перестать общаться с незнакомцем и перезвонить в свой банк или в территориальный орган внутренних дел. Для этого достаточно набрать номер телефона круглосуточной службы поддержки клиентов банка, указанный на Вашей банковской платежной карте или номер 102, и в ходе телефонного разговора прояснить возникшую ситуацию.

Запомните, что ни при каких обстоятельствах нельзя сообщать (передавать) реквизиты банковских платежных карт (номер карты, срок действия, данные держателя, трехзначный код на обратной стороне карты), их фотографии, «логин» и «пароль» доступа к системе дистанционного банковского обслуживания «Интернет-банкинг» и коды доступа к нему в виде SMS-сообщений, поступающих из банка. Указанная информация является конфиденциальной и не подлежит разглашению даже представителям банка и сотрудникам правоохранительных органов.

По причине простоты оформления, мошенники зачастую просят потерпевших оформить кредит путем подачи онлайн-заявки, при оформлении которого не нужно личное присутствие в банке, а также поручители и справки о доходах. Если в дальнейшем потерпевший получает кредитные средства в банке наличными, мошенники под различными предлогами просят его перечислить денежные средства на их счет. В случае получения кредитной карты, злоумышленники выясняют реквизиты данной карты и похищают с нее денежные средства. Есть банки, в которых не обязательно личное присутствие при получении кредита. Кредитные денежные средства могут быть зачислены на действующий счет потерпевшего, к которому привязана банковская карта.

9. БЕЗОПАСНО ПОСЕЩАЙТЕ САЙТЫ В СЕТИ ИНТЕРНЕТ.

Если Вы используете систему дистанционного банковского обслуживания «Интернет-банкинг» для расчетов за коммунальные услуги, денежных переводов, проверки факта зачисления на счет заработной платы (пенсий, пособий и т.п.), Вам необходимо удостовериться в подлинности веб-ссылки, предназначенной для авторизации на интернет-сайте банка.

Дело в том, что кибермошенники временно размещают в сети Интернет веб-ссылки, которые ведут на поддельные (фишинговые) веб-сайты, внешне не отличающиеся от оригинальных.

Пример «фишинговой» ссылки на интернет-банкинг, обнаруженной в результате поискового запроса в браузере «Google».

Подлинная ссылка на веб-сайт интернет-банкинга «Банк БелВЭБ», обнаруженная в результате того же поискового запроса в браузере «Google».

В случае перехода на поддельный веб-сайт, Вам будет предложено ввести «логин» и «пароль» для авторизации. Если Вы это сделаете, то киберпреступники получат доступ к Вашему интернет-банкингу, а находящиеся на банковском счету денежные средства будут похищены. Также Вам не следует переходить по ссылкам, которые Вы получили от неизвестных людей в социальных сетях или мессенджерах. С большой долей вероятности, данные ссылки являются «фишинговыми».

Для безопасного совершения онлайн платежей рекомендуется использовать специальные приложения для мобильных устройств «Мобильный банкинг», которые доступны для скачивания в Google Play Market (для Android) или App Store (для iOS).

10. ИСКЛЮЧИТЕ ВОЗМОЖНОСТЬ КОМПРОМЕТАЦИИ РЕКВИЗИТОВ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТ.

На поверхность банковской платежной карты нанесена информация о номере банковского счета, его владельце, сроке действия карты, трехзначный код (CVV-код). Этих данных достаточно, чтобы производить платежи за товары и услуги в сети Интернет. Утеря банковской платежной карты или ее временное нахождение, даже с Вашего согласия, в распоряжении посторонних лиц создают условия для компрометации ее реквизитов.

Иногда бывает так, что банковскую платежную карту хранят в кошельке вместе с пин-кодом, записанным на ее поверхности или на листке бумаги. В случае утраты кошелька в результате утери или кражи, лицо им завладевшее получает возможность полного доступа к Вашему банковскому счету.

Запомните, что нанесенная на поверхность банковской платежной карты информация является конфиденциальной и не подлежит разглашению посторонним лицам. Не храните Вашу банковскую платежную карту совместно с пин-кодом.

Управление по противодействию киберпреступности криминальной милиции УВД Минского облисполкома