ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

С февраля 2023 года в области отмечается рост количества киберпреступлений. Большинство фактов совершаются методом фишинга.

Количество киберпреступлений в области увеличилось более чем на треть в сравнении с аналогичным периодом прошлого года.

Ущерб, причиненный жителям области за первый квартал текущего года, составляет чуть более 600 тысяч рублей.

Среди жертв киберпреступников представители практически всех сфер деятельности – бухгалтера, экономисты, директора, заместители директоров частных и государственных учреждений, начальники отделов и управлений учреждений, педагоги, врачи и медицинские сестры, студенты ВУЗов, юристы, программисты и представители других специальностей.

Значительную долю киберпреступлений (более 85%) составляют хищения имущества путем модификации компьютерной информации. Основная часть хищений совершается методами фишинга или вишинга.

**ФИШИНГ:** В последнее время вызывает озабоченность рост преступлений методом фишинга – способа, цель которого – завладеть реквизитами банковских платежных карт. Мошенники умело подделывают различные интернет-ресурсы, которые имеют сервис онлайн-платежей, например, банковские услуги, торговые площадки, службы доставки и другие.

Киберпреступники **под любым предлогом вынуждают жертву пройти по ссылке на поддельный интернет-ресурс и ввести на его странице личные данные**: реквизиты платежной карты, логин и пароль к сервису, сеансовые ключи от банка или коды подтверждения.

Пользователи, не замечая подмены, на фишинговых сайтах сами вводят свои персональные данные, после чего данные автоматически попадают злоумышленникам. Владея этими данными, мошенники совершают хищения со счетов.

Из-за временного отсутствия программы некоторых банков в магазинах приложений для мобильных телефонов клиентам чаще приходится пользоваться интернет-банкингом через браузер. При необходимости найти необходимый банк поисковая система может предложить перейти, в том числе, по ссылке и на мошеннический сайт.

Например, belinvestbank.by-salt.com

belinvestbank-by.online

belinvestbank-by.com

beslnvestsbakn.fun

Внешне такой сайт идентичен официальному сайту банка.

Мошеннический сайт от официального **отличить легко**. Во-первых, все интернет-ресурсы белорусских организаций расположены в национальном сегменте Интернета – в домене BY. Адрес главной страницы сайта **должен выглядеть так: «адрес сайта».BY**

Например, belinvestbank.by, mvd.gov.by, vitebsk-region.gov.by, belta.by и другие.

Для других страниц сайта, кроме главной, после последней точки в адресе указывается домен BY, а сразу же за ним наклонная черта, «адрес сайта».BY/\*\*.

Например, belinvestbank.by/individual/credits

belta.by/meteo

*Из значимых таких преступлений за последнее время: Заместитель директора частной организации желал оплатить коммунальные услуги через Интернет, нашел в поисковой системе ссылку с логотипом своего банка, на открытой странице ввел свои логин и пароль к банкингу для входа в личный кабинет. Его данные автоматически передались с мошеннического сайта преступникам и они смогли с его счета перевести более 13  000 рублей.*

*Аналогично, юрист строительной организации перешла по предложенной фишинговой ссылке, ввела на поддельном сайте свои логин и пароль к банкингу, и мошенники похитили у нее 14 000 рублей.*

**Еще один нередкий способ выманивания данных.**

**На сайтах знакомств** мошенники представляются женщинами и заводят виртуальные знакомства с мужчинами. Через непродолжительное время предлагают для личного знакомства вместе сходить в театр, кино или кальянную. Для этого отправляют мужчине **ссылку на поддельный сайт театра (кино, кальянной)**. При покупке билетов мужчина вводит полные данные своей банковской карты, секретный код на обороте, предназначенный для совершения расходных операций, а также проверочный смс-код от банка. Так мошенники завладевают его персональными данными и совершают хищение с банковской карты.

*В Октябрьском РОВД: Мужчина, 24 лет, работающий кладовщиком ветеринарной фабрики, для знакомства с «Альбиной» на сайте БелАрусского театра ввел данные своей карты, после чего потерял все сбережения.*

*Аналогичным способом под предлогом знакомства с «Мариной» похитили денежные средства у студента Витебского университета, врача-хирурга и специалиста в области цифровых технологий.*

*Сайты «театров»:* **beltheatreafisha.store,****kassa-theatre.com, theater.by-shop.online.**

Для белорусских организаций домен должен быть только BY.

**ВИШИНГ:** Мошенники чаще всего используют для совершения преступлений звонки в мессенджерах. Звонящие могут представиться сотрудниками банковских организаций или правоохранительных органов. Под различными предлогами они убеждают произвести какие-либо действия, например, передать конфиденциальную информацию, в том числе смс-коды, оформить кредит или установить мобильное приложение.

Из последних преступлений:

*Неустановленные лица, представившись* ***сотрудниками банка и милиции в*** *общались по телефону в мессенджере Viber с преподавателем ВУЗа из Витебска. Под предлогом аннулирования якобы оформленного неизвестными лицами на ее имя кредита, убедили женщину* ***оформить встречные кредиты*** *на сумму по 10  000 рублей каждый и установить на свой мобильный телефон* ***приложение удаленного доступа****. После чего женщина передала данные своих кредитных карт. В результате неустановленные лица получили доступ к ее счетам и* ***похитили 10 000*** *рублей. Еще 10 000 сумела сохранить сотрудница банка, предупредив ее о таком способе хищений денежных средств.*

*Аналогично женщина, 1975 г.р****., сборщик обуви,*** *поверила звонящим и по указанию незнакомых лиц* ***оформила на себя кредиты*** *в 5 банках, после чего установила мобильное приложение. В результате, сумма похищенных денежных средств составляет более* ***20 000*** *рублей.*

*Аналогичное преступление зарегистрировано в Чашниках. Мужчина по указанию неизвестных* ***установил приложение****, назвал код его регистрации и, в итоге, лишился денежных средств в сумме более* ***22 000******рублей****.*

*Неизвестный, используя мессенджер* ***«Viber»****, представился сотрудником* ***банка****, убедил женщину 1969 года рождения,* ***работающую уборщиком помещений в средней школе Витебска****, оформить на свое имя кредит на сумму* ***8 200*** *белорусских рублей и* ***перевести в четыре этапа*** *денежные средства* ***посредством платежного терминала*** *на банковский расчетный счет, после чего похитил их.*

*Сотрудница Белорусской железной дороги под напором мошенников в ходе разговора в мессенджере перевела на указанные ей счета почти 36 000 рублей, взятых в кредит в 5 разных банках.*

**Чтобы не стать жертвой киберпреступника:**

1. Не выполняйте никаких действий по просьбе незнакомых лиц: не оформляйте кредиты и не устанавливайте непроверенные программы.
2. Пользуйтесь мобильными приложениями (банков, торговых площадок, сервисов услуг).
3. В браузере переходите в интернет-банкинг только с главной страницы банка, для этого нужно кликнуть на разные ссылки (например, курсы валют, кредиты, вклады и т.д.).
4. Всегда проверяйте адрес и доменное имя сайта, где вводите личные данные. Для белорусских организаций домен должен быть только BY. Для разделов сайта, кроме главной страницы, после BY должна быть наклонная черта.
5. Активируйте на карте услугу 3-D Secure (подтверждение платежей кодом из смс от банка).

**Набирает обороты НОВЫЙ ВИД** **ВОВЛЕЧЕНИЯ** в преступную деятельность. Гражданам предлагают за вознаграждение оформить на свое имя банковские карты и любым способом передать третьим лицам их реквизиты. Преступники уверяют, что за такие деяния нет никакой ответственности, но это не так. Часто на такие уловки попадаются молодые люди, которые находят подработку в Интернете, и те, кто не имеет постоянного дохода, живет за счет случайных заработков.

Надо знать, что **такие действия влекут за собой уголовную ответственность по ст. 222 УК РБ** за незаконный оборот средств платежа.

Имеются факты, когда в преступную деятельность были вовлечены мать троих детей, 20-ти летняя девушка, мужчина, не имеющий постоянного дохода, учащиеся колледжа.

*В Шарковщине женщина не догадывалась, что стала звеном преступной киберцепочки. Всего за неделю через ее карт-счет преступники провели более 74 000 рублей. Ее сын нашел подработку в сети и «сбросил» заказчикам паспортные данные и смс-коды с телефона матери. Благодаря этому мошенники сумели создать виртуальную карту, через которую выводили похищенные у доверчивых граждан деньги.*

Кроме вышеперечисленного, киберпреступления **совершаются**   
**В ОТНОШЕНИИ ЮРИДИЧЕСКИХ ЛИЦ**. Бывает так, что цель хакеров – получить доступ к конфиденциальной информации, но чаще всего атакующих интересуют деньги. Может использоваться взломанная электронная почта предприятия-партнера, тогда злоумышленники продолжают переписку с сотрудником предприятия или организации с целью завоевать его доверие и убедить выполнить некоторые действия в интересах самих злоумышленников.

*К примеру, в сентябре 2022 года на электронный почтовый ящик сотрудника одного из предприятий г. Витебска поступило электронное письмо от партнера из Кореи, к почте которого получен несанкционированный доступ. Письмо содержало информацию об изменении расчетного счета и информацию об образовании дочернего предприятия. Также письмо содержало требование оплатить доставку товара на новый расчетный счет. В последующем, данный сотрудник подготовил дополнительное соглашение, содержащее измененные реквизиты счета для оплаты товара, а после его подписания руководством (в октябре 2022 года) денежные средства в сумме* ***более 24 420 долларов*** *зачислены на расчетный счет злоумышленника, открытый в банковском учреждении Китая.*

*Аналогично, сотрудники других предприятий Витебска переводили на указанные им в переписке расчетные счета по 20 000 и 30 000 долларов.*

Также мошенники могут использовать адрес, который визуально похож на официальный адрес субъекта хозяйствования или его партнера, но отличается на несколько символов (БЕЗ ВЗЛОМА ПОЧТЫ ПАРТНЕРА).

*Еще пример: «kula@telliko.com», вместо «kula@te1liko.com».*

Зачастую преступление состоит из нескольких этапов.

*В декабре 2022 года злоумышленники создали фишинговый сайт нефтеперерабатывающего предприятия, аналогичный оригинальному, зарегистрировали его с похожим Интернет-адресом и от имени белорусского предприятия вели переговоры с заинтересованными о поставках несуществующих продуктов переработки, не имея на то возможности. В итоге, получили деньги на подконтрольные им счета.*

Планируя кибератаку, злоумышленники прежде всего рассчитывают на человеческие ошибки и слабости, а не уязвимость программного обеспечения, которую гораздо сложнее преодолеть.

Необходимо понимать, что мошенник не сможет достичь своей цели и похитить денежные средства, если атака будет своевременно выявлена и остановлена, а это возможно на любом ее этапе при соблюдении работниками элементарных правил цифровой гигиены.

Управление по противодействию киберпреступности

криминальной милиции

УВД Витебского облисполкома