НЕДЕТСКИЕ ИГРЫ 2.0

КАК НЕ СТАТЬ УЧАСТНИКОМ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

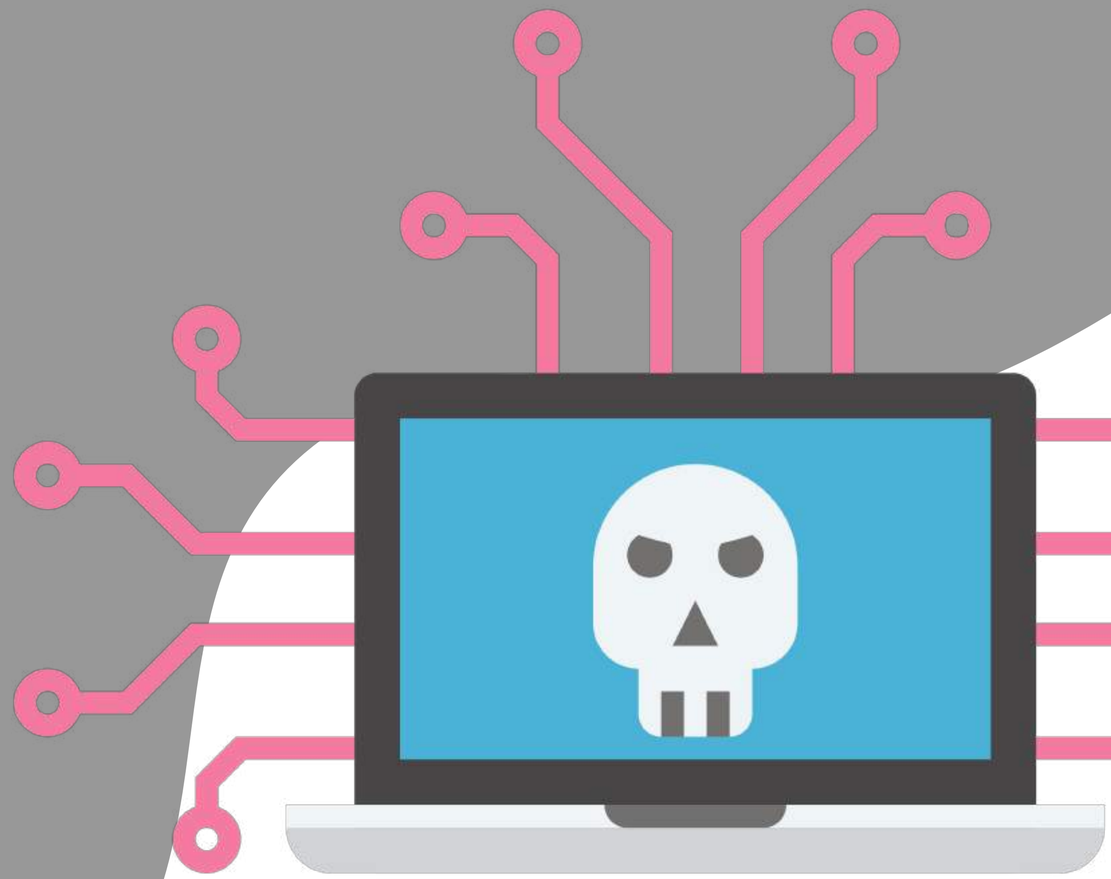
ТЕМАТИЧЕСКИЙ УРОК

ДРОППЕРЫ

это лица, которые используют свои карты для обналичивания или транзита (дальнейшей отправки) похищенных денежных средств

ПОПУЛЯРНЫЕ СПОСОБЫ ВЫВОДА ДЕНЕГ

1. перевод в криптовалюту сразу с карты потерпевшего, с т.е. так называемого «грязного» пластика
2. перевод в криптовалюту с «чистого пластика», т.е. взнос денежных средств на карты дропа, которая ранее не участвовала в сомнительных операциях
3. обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой криптовалюты
4. обналичивание, аккумулирование крупных денежных сумм, с последующей покупкой валюты
5. обналичивание крупных денежных сумм, транспортировка в другой регион взнос на «чистый» пластик и далее межбанковские переводы



115-ФЗ

«О ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЁМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА»

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Согласно статистике, 80% хищений средств происходит дистанционно, более того ежегодно растет не только количество преступлений, но и объем похищенных средств

СИТУАЦИЯ

Людмила является активным клиентом одного из крупнейших федеральных банков страны, где имеет зарплатную карту, накопительный счет, вклад и другие банковские продукты. Людмила решила инвестировать накопившиеся сбережения в строящееся жилье. Ввиду современных трендов предполагалась цифровая сделка, то есть подписание ДДУ (договор долевого участия) с помощью УКЭП (усиленная квалифицированная электронная подпись), являющейся электронным аналогом рукописной подписи. Пока Людмила ожидала «выпуска» УКЭП, ей поступил звонок от «сотрудника» Госуслуг, который ей сообщил, что на ее имя было получено письмо. Злоумышленник уточнил, какой способ передачи письма наиболее удобен: посредством электронной почты или отправкой на домашний адрес, который к тому же был назван мошенником корректно. Людмила, не заподозрив подвоха, попросила направить письмо на адрес электронной почты (для ускорения процесса). Для этого «сотрудники» Госуслуг направили на ее телефон смс-код и попросили его продиктовать. Только через 10-15 минут, после того как смс-код был назван, женщина решила еще раз внимательно прочитать направленное ей сообщение и обнаружила, что в его содержании есть информация о смене пароля на портале Госуслуг. При попытке зайти в свой ЛК на Госуслугах она увидела, что доступ был уже более невозможен. Очевидно, что произошла смена пароля

Сотруднику одного из вузов города Москвы в Telegram пришло сообщение от ректора этого вуза о том, что в отношении образовательного учреждения проходит проверка со стороны правоохранительных органов в части распространения персональных данных. «Ректор» пояснил, что ранее сам он уже общался на данную тему и предупредил сотрудника о том, что скоро поступит звонок от представителя МВД. Далее, как было сказано ранее, с сотрудником связался представитель правоохранительных органов с сообщением о том, что от имени жертвы проводятся незаконные финансовые операции и для сохранности сбережений на время следствия необходимо перевести свои деньги на «специальный» счет

Самым лучшим вариантом противодействия такому виду мошенничества будет завершение контакта и связь с руководителем посредством городского или мобильного телефона по своей инициативе

СИТУАЦИЯ

Мужчине по имени Павел после рабочего дня раздался звонок с неизвестного мобильного номера. Павел как деловой человек, которому часто звонят по рабочим вопросам, ответил. Звонящий представился сотрудником мобильного оператора (при этом не уточнил, какого именно) и любезно сообщил о том, что если срок действия договора мобильной связи не продлить в тот же день, то сим-карта прекратит работу и данный номер продадут новому владельцу. Павел уточнил у «сотрудника» мобильного оператора, что нужно сделать для продления договора. Ему ответили, что договор можно продлить «прямо сейчас» в режиме телефонного звонка и никакие персональные данные не потребуются, поскольку они были переданы «ранее при оформлении сим-карты». Однако мошенники попросили продиктовать смс-код, который поступит на телефон. Так как Павел уже знал о подобных схемах, то он прервал разговор, положив трубку

1

Поступившее смс-сообщение якобы для продления договора на самом деле будет являться сбросом пароля для портала «Госуслуги» (о чем рассказано выше). Злоумышленники могут получить исчерпывающую информацию для дальнейших махинаций, например, для оформления кредитов в МФО (микрофинансовых организациях).

2

«Сотрудники» оператора для продления договора мобильной связи попросят ввести определенную комбинацию цифр на телефоне, что приведет к переадресации входящих вызовов и смс сообщений на мобильные телефоны мошенников и может дать им полный карт-бланш для смены паролей, в том числе в банковских приложениях.

ЗАПОМНИТЕ, ЧТО ОПЕРАТОРЫ СОТОВОЙ СВЯЗИ НИКОГДА НЕ БУДУТ ПРОСИТЬ ПРОДИКТОВАТЬ СМС-КОД И НИКОГДА НЕ ПОПРОСЯТ ПРОДИКТОВАТЬ ВАШИ ПАСПОРТНЫЕ ДАННЫЕ

СИТУАЦИЯ

Жертва получает анонимную доставку цветов или некого подарка, что вызывает приятное удивление. На следующий день жертве поступает звонок с сообщением от службы доставки, что курьер не отчитался за данную доставку установленным образом, и просьбой продиктовать «код подтверждения доставки»

Важно никогда не принимать от курьеров заказы, которые не были оформлены лично или о которых вы не уведомлены

СИТУАЦИЯ

Женщина из Москвы решила сдать свою квартиру в аренду. Для повышения стоимости она решила ее меблировать и приобрести шкаф на сервисе «Авито». Подобрав понравившуюся позицию, она связался с продавцом и договорилась о цене в размере 10 000 рублей. Он предложил ей самой заказать доставку, направив фишинговую ссылку на популярный сервис «Яндекс-доставка». Женщина прошла по ссылке (важно отметить, что страница сервиса выглядела, как ее оригинал), ввела нужный адрес доставки и данные своей банковской карты для оплаты. В этот момент с карты москвички была списана сумма 10 000 рублей, но на сайте произошел сбой, и сервис попросил ввести данные карты еще раз для возврата денежных средств. После повторного ввода данных с ее карты вновь была списана сумма в том же размере 10 000 рублей.

ОСНОВНОЕ ПРАВИЛО ФИНАНСОВОЙ БЕЗОПАСНОСТИ ДОСТАТОЧНО ПРОСТОЕ:

НЕ ОТВЕЧАТЬ НА ЗВОНКИ С НЕЗНАКОМЫХ НОМЕРОВ

Возможности искусственного интеллекта в реализации преступных схем

СОЗДАНИЕ ПОДДЕЛЬНОГО ВИДЕО

Создание дипфейка

Мошенники использовали технологии глубокого обучения для создания видео, имитирующего действия генерального директора компании. Они смогли сделать так, чтобы видео выглядело очень правдоподобно, используя открытые источники, такие как видеозаписи публичных выступлений и интервью генерального директора.

Обман

С помощью полученного дипфейка мошенники связались с одним из филиалов этой компании, представляясь генеральным директором. Они использовали видео, чтобы убедить сотрудников в том, что им необходимо сделать срочный перевод средств на «специальный счет».

Вымогательство

В результате манипуляций мошенников сотрудники филиала сделали перевод значительной суммы денег, полагая, что руководство компании действительно дало такое указание

Раскрытие мошенничества

Когда стало очевидно, что денежные средства не были переведены по легальным причинам, компания начала расследование. В ходе расследования было выяснено, что видео было фальшивым, и это привело к осознанию того, как технологические новшества могут быть использованы в преступных целях.

«ГЛУБОКОЕ ПОДДЕЛЫВАНИЕ ГОЛОСА» (VOICE SPOOFING)

ПРИМЕРЫ:

- создание подделки голоса
- фейковый звонок с просьбой о помощи
- вымогательство средств

СБОР ИНФОРМАЦИИ О КОМПАНИИ И/ИЛИ О ЧЕЛОВЕК ПЕРЕД «ВЗЛОМОМ»

- создание фальшивого профиля
- осуществление мошеннического запроса
- выполнение перевода
- раскрытие мошенничества

Обнаружение вредоносного ПО. Машинное обучение

ОБНАРУЖЕНИЕ ПО СИГНАТУРАМ

ГЕНЕРАЦИЯ ВРЕДОНОСНОГО КОДА

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИИ ДЛЯ АДАПТАЦИИ АТАК

АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ГЕНЕРАЦИЯ АТАКИ С ИСПОЛЬЗОВАНИЕМ ИИ

ФИЗИЧЕСКОЕ РАСПРОСТРАНЕНИЕ

ВАЖНО!

1. Активируйте многофакторную аутентификацию на всех значимых аккаунтах, таких как банковские приложения, портал «Госуслуги», личный кабинет Федеральной Налоговой Службы и другие.
2. Закройте доступ для посторонних лиц в социальных сетях, следите за цифровым следом, который вы оставляете в сети Интернет.
3. Критически относитесь ко всему, что видит и слышите.

ДРОППЕРЫ/ДРОПЫ: СВЯЗУЮЩЕЕ ЗВЕНО ПРЕСТУПНОЙ ЦЕПИ ФИНАНСОВЫХ МОШЕННИКОВ

Дропы являются соучастниками преступлений, которые могут быть классифицированы по статье 174 УК РФ Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем или по статье 159 УК РФ Мошенничество

Дропы – это подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт граждан. Стоит отметить, что дропы не являются организаторами преступлений, но являются их соучастниками, за что несут полную ответственность перед законом.

*По данным «Сбера», в дропперство вовлечено порядка **2 млн россиян** – это почти в два раза больше, чем в 2023 году. **Около 60%** – молодые люди до 24 лет, для которых характерно стремление к легкому заработку*

Примеры вербовки дропперов

Студент по имени Андрей хочет заработать денег в свободное время. На сайте по поиску работы ему подвернулась заманчивая вакансия со следующими требованиями: без опыта работы; удаленно; частичная занятность; высокий заработок за несколько часов в день; возраст 18+ и наличие карты любого банка.
Те, кто откликается на подобные вакансии, почти всегда становятся участникам мошеннических схем. Мошенники придумывают различные легенды, например, представляются крупной компанией, занимающейся поставками большого количества товаров из Китая. С учетом крупных сумм покупок и лимитами банков на ежемесячные переводы в компанию требуются люди, которые «отдадут» в аренду свою банковскую карту вместе с личным кабинетом для контроля поступления денег от «клиентов» за вознаграждение.

«КУРЬЕР НАЛИЧНОСТИ»

перемещение денежных средств от одного лица или бизнеса к другому, с целью избежать традиционных банковских методов или при наличии ограничений на вывод. объявление о такой работе размещается телефонными мошенниками, при этом будущему курьеру могут сообщать, что работа не связана с криминалом и он ничем не рискует.

ПРИМЕР

Нужны ответственные люди по всем городам РФ;
Работа курьером;
Забираем посылки от 100 тыс. руб.
Даем 7%, выплата сразу;
Вся «почва» для безопасного забора нала подготовлена!!!

ВАЖНО!

ст. 159 УК РФ. Наказание в этом случае предусмотрено вплоть до 10 лет лишения свободы

СИТУАЦИЯ

На ваш счет поступает перевод денег от незнакомого лица, далее вам поступает звонок с информацией, что денежный перевод был совершен ошибочно, и просьбой перевести деньги обратно. Однако в случае возврата по указанным незнакомцем реквизитам на самом деле деньги направляются третьему лицу – участнику преступной схемы. Таким образом, случайно, пойдя навстречу человеку, можно стать соучастником преступления по выводу денег.

В данном случае правильным решением будет обратиться в банк и только вместе с банковским сотрудником решать вопрос, каким образом деньги отправить обратно.

ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ И САЙТЫ ЗНАКОМСТВ

Через социальные сети обращается незнакомец с правдоподобной легендой, например, что у него есть родственник за границей, которому срочно нужно отправить деньги, а его банк такие переводы не проводит. Обычно мошенники предлагают это сделать за небольшую плату в зависимости от суммы предполагаемого перевода. Далее на счет жертвы поступают ворованные деньги, которые она перенаправляет дальше, становясь таким образом звеном в преступной цепочке.

ВОВЛЕЧЕНИЕ В ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ

Работа с уязвимыми группами – привлечение людей, испытывающих финансовые трудности

«Борьба за правое дело» - злоумышленники занимаются пропагандой через социальные сети, обещая участие в «правой войне»

Подрыв доверия к государству – мошенники призывают действовать против «несправедливой системы»

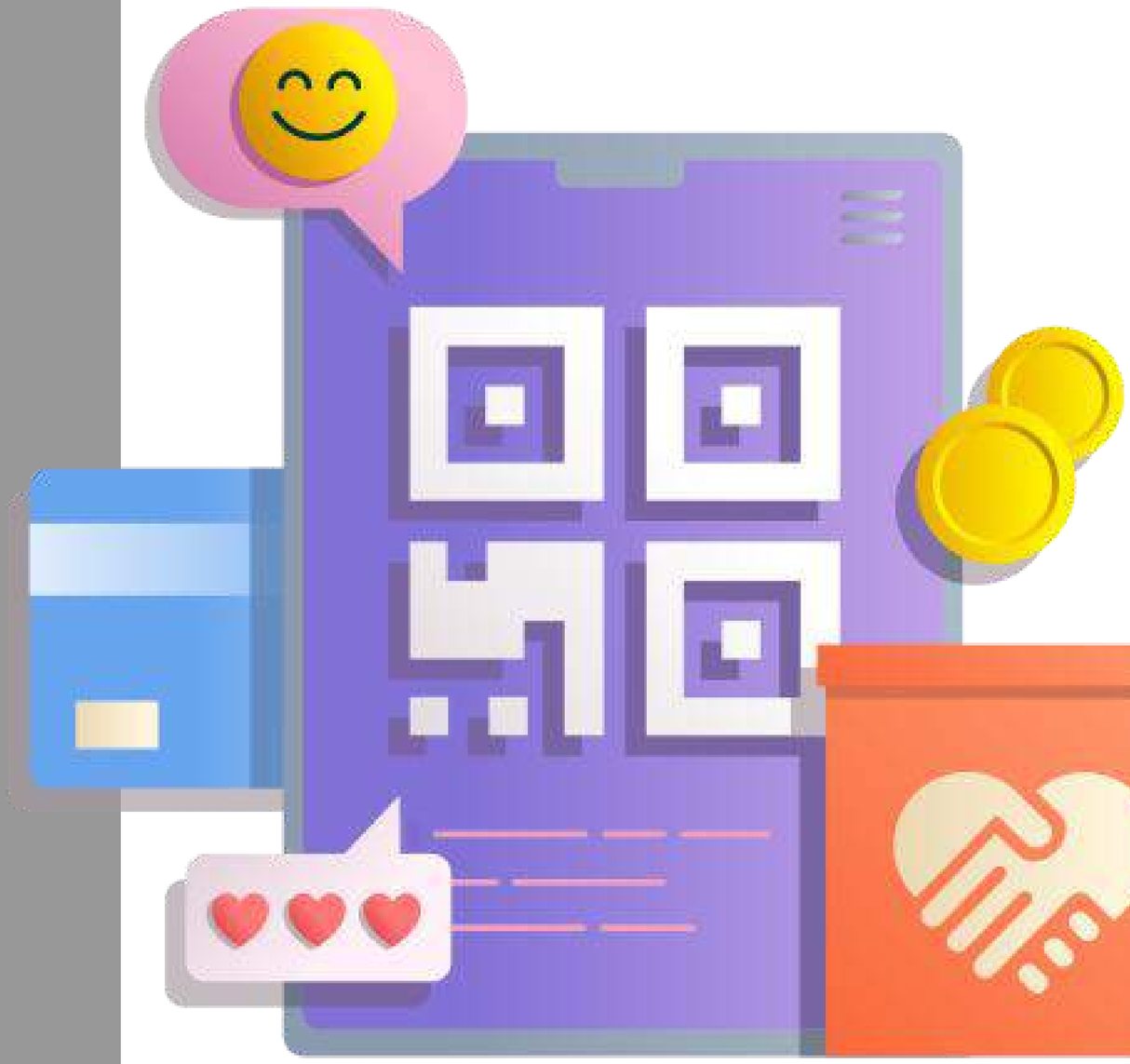
Обеспечение наркотиками – вербовщики делают людей зависимыми от наркотиков и склоняют их к диверсионным действиям

ВАЖНО!

За совершение диверсии наступает уголовная ответственность в виде лишения свободы на срок от 10 до 20 лет лишения свободы.

БЛАГОТВОРИТЕЛЬНЫЕ СБОРЫ ДЛЯ СВО/ПРИЮТ ДЛЯ ЖИВОТНЫХ/НА ОПЕРАЦИЮ

Мошенники создают благотворительный фонд, например, для помощи студентам вузов, попавшим с сложную жизненную ситуацию; и на счет созданного фонда те организации, которым необходимо легализовать преступные средства, перечисляют деньги



ОБМЕН КРИПТОВАЛЮТЫ НА РУБЛИ

ПРАВИЛА РАБОТЫ С КРИПТОВАЛЮТОЙ

- вести переписку через инфраструктуры p2p площадки
- совершать сделки с аккаунтами, которые давно зарегистрированы на площадке и имеют хорошую репутацию

ВАЖНО!

Важно помнить, что самые безопасные сделки проводятся на криптобиржах

ОБНАЛЬЩИКИ

*это дропы, которые **снимают со своей карты** преступные деньги и передают их мошенникам.*

ТРАНЗИТЧИКИ

*это дропы, которые **пересылают безналичным путем** преступные деньги по указанным мошенникам реквизитам.*

ЗАЛИВЩИКИ

*это дропы, которые получают наличные деньги от таких же дропов, **вносят их на свою карту** и пересылают дропам «транзитчикам».*

УНИВЕРСАЛЫ

*это дропы, которые могут выполнять **все вышеуказанные действия**.*

Важно отметить, что суровость наказания не зависит от того, знал ли дроп о том, что он делает, или нет

ПРАВИЛА БЕЗОПАСНОСТИ

- не откликайтесь на вакансии с легким заработком. когда обещается легкий и при этом высокий заработок, то это точно мошенническая схема
- потенциального работодателя проверяйте на предмет наличия отзывов в интернете
- никогда и никому не оставляйте данные своей банковской карты, тем более не передавайте ее третьим лицам (во многих банках передача карт третьим лицам запрещена)
- регулярно обновляйте пароли к своим банковским приложениям, личному кабинету портала «госуслуги» и прочим финансово значимым приложениям
- не переходите по ссылкам из неизвестных источников, во избежание взлома доступа к банковскому личному кабинету
- всегда повышайте свою финансовую грамотность – читайте новости о новых видах мошенничества, ведь «предупрежден – значит вооружен»
- если вас попросят вернуть случайный перевод денег, совершенный на ваше имя, не соглашайтесь на это, обратитесь с этим вопросом в ваш банк

Только тихо!
Всё об анонимности криптовалют

ВЫВОД СРЕДСТВ ИЗ КРИПТОВАЛЮТНЫХ ОБМЕННИКОВ И БИРЖ

Криптобиржи

это более сложная структура, которая предполагает регистрацию и часто необходимость пройти процедуру «Знай своего клиента». Ключевым отличием от криптообменников является возможность торговать на бирже своими активами, а не просто обменивать.

Криптообменники

Онлайн криптообменник предоставляет возможность быстрого обмена криптовалюты. Достаточно выбрать валюту, которую вы хотите продать, и валюту, которую хотите купить. После ввода своих данных вы получаете нужные средства на свой кошелек.

ОСНОВНЫЕ ТИПЫ ПРЕСТУПЛЕНИЙ С КРИПТОВАЛЮТАМИ

МОШЕННИЧЕСТВО

В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с гражданкой «М» связалась девушка, которая, используя методы социальной инженерии убедила «М» приобрести криптовалюту и инвестировать её на бирже «С». В ходе финансового расследования МРУ Росфинмониторинга по СКФО установило, что сайт биржи был подделкой, а криптовалюта, вложенная потерпевшей, выводилась преступниками на одну из известных криптобирж, обменивалась на стэйблкойны и в дальнейшем переводилась на анонимные криптокошельки

ПРОГРАММЫ-ВЫМОГАТЕЛИ (RANSOMWARE)

Одна из крупнейших атак осуществлена на компанию Colonial Pipeline. в 2021 году. Вымогатели потребовали оплату в биткойнах на сумму около 4,4 млн долларов. После получения выкупа преступники пытались скрыть свои средства, разбивая транзакции на мелкие части и переводя их через различные криптовалютные кошельки для запутывания следов

КИБЕРПРЕСТУПЛЕНИЯ И ВЗЛОМЫ

Наиболее известные случаи взлома криптовалютных бирж, такие как взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, привели к огромным потерям.

НАРКОТОРГОВЛЯ И ИНАЯ НЕЛЕГАЛЬНАЯ ТОРГОВЛЯ

В качестве примера можно привести платформу Hydra, деятельность которой была пресечена в 2022 году. По имеющимся данным Hydra контролировала более 90% незаконной торговли в даркнете, где за все товары и услуги, включая наркотики, оружие и поддельные документы, оплачивались криптовалютой

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА

Криптовалюты также используются для финансирования террористических организаций, так как они позволяют совершать анонимные переводы без необходимости использовать традиционные банковские системы.

ПРАВИЛА БЕЗОПАСНОСТИ

используйте двухфакторную аутентификацию

храните резервные копии в безопасных местах

используйте сложные пароли

желательно использовать отдельное устройство только для доступа к кошелькам

регулярно обновляйте программное обеспечение

позаботьтесь о защите своего устройства

не афишируйте в публичных местах наличие большого количества криптовалюты на ваших кошельках

МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ФИНАНСОВОМУ МОНИТОРИНГУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУДН

МУМЦФМ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

ЦЕНТР МЕЖОЛИМПИАДНОЙ ПОДГОТОВКИ

содружество

Т БАНК

Альфа-Банк

Цели Олимпиады:

- повышение общей информационной, финансовой и правовой грамотности молодежи, формирование новой формы мышления и нового формата деятельности, выявление талантливых школьников и студентов в области финансовой безопасности;
- создание условий для индивидуальной образовательной траектории, содействие профессиональной ориентации школьников и студентов для формирования кадрового ресурса системы финансовой безопасности;
- стимулирование учебно-познавательной и научно-исследовательской деятельности школьников и студентов, развитие научных знаний в области финансовой безопасности.