ПАМЯТКИ ДЛЯ РОДИТЕЛЕЙ И ДЕТЕЙ
КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ И НЕ СТАТЬ СОУЧАСТНИКОМ ПРЕСТУПЛЕНИЯ

САМЫЕ ПОПУЛЯРНЫЕ СХЕМЫ МОШЕННИЧЕСТВА

Выпускники школ – в центре внимания. Продажа «ответов» на задания ЕГЭ. Получив деньги, мошенники отправляют варианты прошлых лет или просто перестают отвечать жертве.

Аферисты создают фейковые сайты и группы в соцсетях, выдающие себя за приемные комиссии высших учебных заведений. Абитуриентам предлагают купить якобы бюджетные места, после получения денег злоумышленники пропадают.

Сообщения от неизвестных в мессенджере о том, что камера видеонаблюдения якобы зафиксировала списывание на ЕГЭ. Выпускнику предлагают выкупить запись. После перечисления средств связь обрывается, аккаунт мошенника блокируется.

Ваш отпуск под угрозой... Злоумышленники предлагают липовые туры, бронирование билетов и жилья якобы по выгодным ценам.

Всегда внимательно проверяйте правильность написания названия сайта и пользуйтесь услугами проверенных компаний.

Концерта нет, а билеты есть! Мошенники создают фишинговые сайты с афишей несуществующего выступления и заманивают туда потенциальных жертв.

Также фиксируется рост числа фишинговых сайтов, на которых аферисты предлагают заказать букеты, конфеты, парфюм и другие подарки якобы по оптовым ценам или с большими скидками.

«Моя племянница участвует в конкурсе...». Одним из самых распространённых способов по угону аккаунтов в соцсетях и мессенджерах стали сообщения с просьбой проголосовать за ребенка, который участвует в каком-то конкурсе, а на кону – ценный приз.

Такие сообщения обычно приходят от кого-то из списка ваших контактов, к чьей учетной записи уже получили доступ аферисты.

Переходя по ссылке для «голосования», вы попадаете на фишинговый сайт. Чтобы отдать свой голос, вас попросят авторизоваться. Если вы введете данные для входа в профиль, их получат злоумышленники.

Действие вашей SIM-карты истекает? Телефонные мошенники обзванивают россиян под видом сотовых операторов с предложением продлить якобы истекающий договор на номер телефона.

В ходе разговора абоненту приходит сообщение с кодом, который необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок». Этот код – данные для входа в личный кабинет жертвы на портале «Госуслуги» или на других сервисах.

В действительности договоры, заключаемые абонентом с сотовыми операторами, бессрочные!

Ваш голос могут украсть. Злоумышленники активно используют нейросети. С их помощью они могут прислать голосовое и даже видеосообщение от имени вашего друга, которого взломали.

Также будьте внимательны с предложением о платной озвучке рекламы и фильмов, которую распространяют злоумышленники в сети. Собранные экземпляры голосов аферисты используют для обучения нейросетей и генерируют на их основе аудиосообщения, с помощью которых потом вымогают деньги у друзей и родственников жертвы.

На связи ваш «начальник». Злоумышленники звонят и пишут в мессенджере пользователям под видом их начальников с работы. Для этого они создают реалистичные профили руководителей. Аферист сообщает жертве о каких-то проблемах и о том, что с ним свяжется «сотрудник» правоохранительных органов.

Второй мошенник в разговоре убеждает гражданина разными способами в том, что его деньги хотят украсть, перевести на счета СБУ или оформить на его имя кредит.

Вариаций много, но «спасительный ход» один – вывести деньги на «безопасный счет».

Фейковые электронные письма от госведомств. Пользователи получают электронные письма якобы от ФНС России, Роскомнадзора и других ведомств, в которых обычно говорится о каком-то «нарушении» со стороны жертвы или иной «проблеме». С помощью такой рассылки аферисты заманивают россиян на фишинговые сайты, собирают персональные данные или распространяют зараженные вирусами файлы.

НЕ ДАЙТЕ РЕБЕНКУ СТАТЬ ДРОППЕРОМ

В последнее время мошенники активно втягивают подростков в свои схемы. Например, используют их в качестве дропперов. Школьники и студенты, желая заработать деньги, соглашаются на условия преступников.

Дропперы — подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт посторонних людей.

Например, можно наткнуться на рекламу банка, где предлают завести карту и обещают за это заплатить — надо только сообщить потом данные этой карты менеджеру. Так банк якобы выполняет план по продажам.

Объявление заманчивое, вроде бы делать ничего особенного не нужно, плюс денег на карте нет, тогда в чем подвох?

А подвох в том, что, зная данные карты, можно офомить "левый" кредит или использовать банковский счет для мошеннических операций с деньгами. Полиция потом не найдет следов, а придет за объяснением к владельцу карты.

Поэтому очень важно объяснять подросткам, что быстрых и легких денег не бывает. Если из вакансии непонятно, чем именно нужно заниматься, не требуется опыт работы и есть фразы наподобие «Минимум усилий», «Ежедневные выплаты», «Доход не ограничен» — это опасные сигналы.

ПРАВИЛА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ ДЛЯ ДЕТЕЙ:

1. Советоваться с родителями. Перед регистрацией на сайте, созданием профиля в социальной сети и выкладыванием фотографий рекомендуется посоветоваться с родителями.

2. Беречь личные данные. Не нужно рассказывать подробности о себе и о родителях.

3. Не делиться информацией о знакомых. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают.

4. Фильтровать информацию. Не стоит слепо доверять всему, что пишут в интернете.

5. Проверять данные. Можно поискать ту же информацию в других источниках, чтобы сравнить детали и способ ее подачи.

6. Не общаться с чужими людьми. Любая назойливость, частые обращения, просьбы что-то написать и тем более прислать фото — это повод для того, чтобы сразу же прекратить общение и заблокировать человека.

7. Придумывать сложные пароли. Простой пароль легко запомнить, но его очень просто взломать.

8. Обращать внимание на сайты. Важно быть внимательным и обращать внимание на детали, в частности на адрес сайта.

9. Уметь отличать поддельные аккаунты.

10. Помнить о вежливости. В любой ситуации, даже если кажется, что это обман, не стоит грубить и тем более использовать нецензурную лексику.

Мошенники обманывают детей, играющих в Roblox, обещая им валюту (робуксы) или предметы для популярной онлайн-игры.

Суть схемы: аферисты могут уговорить детей, зарегистрированных в группах по раздаче робуксов, самостоятельно перевести им родительские деньги в обмен на игровые бонусы. Свои действия злоумышленники маскируют под «задания».

Также мошенники могут действовать иначе. Они предлагают «помощь» детям в покупке виртуальной валюты и просят подростков передать им данные банковских карт кого-то из родителей, или взять телефон взрослого и следовать указаниям. Такое общение чаще всего происходит в мессенджерах и не приводит ни к чему хорошему: игроки остаются без бонусов, а их родители — без средств на счетах.

Расскажите своим детям о рисках общения с незнакомыми в интернете и запретите им передавать личные данные в обмен на какие-либо бонусы.

В социальных сетях и мессенджерах провокаторы склоняют россиян к терроризму и другим серьезным преступлениям. В группе риска – подростки и молодежь.

Вовлекать юных граждан в террористическую деятельность злоумышленникам намного легче, чем заставить сделать нечто противозаконное зрелого человека. Личностная незрелость, отсутствие жизненного опыта, непонимание глубинных политических процессов сливается с излишней эмоциональностью, импульсивностью, желанием

проявить себя, почувствовать свою принадлежность к группе. В силу свойственной этому возрасту самоуверенности они чаще склонны считать, что могут не попасться правоохранительным органам и уйти от ответственности.

Большинство вербовщиков – тонкие психологи, обученные техникам и методикам воздействия на психику людей. Для вербовщиков не существует «грязных» методов – сгодится все, что может способствовать их делу. Спектр воздействия чрезвычайно широк: от психологических манипуляций и пропаганды до прямых угроз и шантажа.

Главным инструментом вербовки в террористские организации в современное время стали социальные сети и мессенджеры, основными потребителями контента которых является молодежь.

Для подростков и молодых людей свойственно вести свои страницы открыто, они чаще публикуют персональную информацию, демонстрируют те или иные свои взгляды, ярко реагируют на тот или иной политический или околополитический контент, при этом не всегда могут отличить фейковые новости от реальных.

Соцсети позволяют провокаторам свободно собирать интересующие их данные и еще на этапе планирования «вербовки» анализировать личные страницы потенциальных жертв, выбирая тех людей, которые демонстрируют активность, определенные политические, религиозные или иные взгляды, и в то же время не имеют четких личностных позиций.

РОДИТЕЛЯМ ВАЖНО:

- заранее проинформировать детей и подростков обо всех возможных рисках и угрозах сети Интернет, в том числе о наличии активной деятельности по вербовке в террористические организации;

- научить ребенка не отвечать на сомнительные предложения и сообщения в социальных сетях и быть подозрительным, если требуют сохранить тайну переписки (общения) и не сообщать родителям;

- спрашивать или аккуратно проверять с кем ведёт переписку ребёнок в личных сообщениях;

- обращать внимание на поведение и новые интересы ребёнка: аниме, депрессивная литература, специализированные книги об оружии и стрельбе;

- обращать внимание, если ребенок в реальной жизни выполняет задания, полученные в Интернете, так называемые, челленджи. Они могут содержать опасные для здоровья действия;

- создавать семейные традиции, возможности для получения позитивных эмоций вне Интернета (путешествия, выставки, музеи, походы, праздники, творчество, хобби), комфортные условия проживания и позитивные взаимоотношения с ребенком;

- поддерживать контакты с друзьями и одноклассниками ребенка, а также их родителям.

КАК РЕАГИРОВАТЬ ПОДРОСТКУ?

- сообщать о любых предложениях и (или) подозрительных новых знакомых родителям или педагогам;

- прежде чем репостить какую-то информацию в социальной сети, проверьте на сайте Министерства юстиции Российской Федерации, вдруг она внесена в список запрещённых;

- сообщить в правоохранительные органы (тел. 102).

Посредством социальных сетей и мессенджеров злоумышленники вербуют детей для совершения преступлений, в том числе террористического характера!!

Поскольку знакомство в сети Интернет протекает легче, чем в реальности, своих жертв вербовщики находят в основном в социальных сетях и на сайтах знакомств.

Первичный отбор «кандидатов» осуществляется по исследованию информации, которую дети выкладывают на своих личных страничках в социальных сетях.

Фотографии, записи на стене, комментарии, участие в группах дают представление об интересах человека, круге его общения, комплексах и проблемах и служат «сокровищницей» для психоанализа и набора наиболее подходящих для вербовки личностей.

О ЧЕМ НУЖНО ЗНАТЬ, ЧТОБЫ НЕ ПОПАСТЬ ПОД ВЛИЯНИЕ ПРОВОКАТОРОВ:

1. Не размещать на своей страничке информацию о месте своего жительства и местах работы родителей.

2. Не отвечать на вопросы незнакомых людей.

3. Ограничить доступ к своим фотографиям, записям и другим материалам только кругом хорошо знакомых людей.

4. Не откровенничать в общедоступных группах и на форумах.

5. Не вступать в споры. Агитаторы привлекают внимание людей темами, вызывающими споры. Потом выходят на связь с теми, кто принял участие в обсуждении, и призывают в свои ряды.

6. Не принимать в друзья всех подряд.

7. Быть внимательным и всегда стараться выяснить личность того, кто проявляет интерес к общению либо обстоятельства возможного раннего знакомства.

8. Если пришло сообщение непонятного содержания с незнакомого номера, не отвечать на него. Опция «Черный список» позволяет заблокировать любого человека, который досаждает какими-то вопросами.

9. Использовать возможность пожаловаться модератору или администратору сайта.

Мошенничества с банковскими карточками становятся более изощренными, к ним специально привлекают подставных людей. Рассказываем, кто такие дропы и почему они могут получить до тысячи долларов и до семи лет лишения свободы за один день.

Деятельность дропперов нелегальна.

Если вы недавно искали работу, то наверняка находили на различных специализированных платформах подозрительно заманчивые предложения: предлагают зарабатывать много денег за короткий срок и за минимум усилий, не выдвигают особых требований к кандидату и принимают без опыта. Будьте внимательны: под такой вакансией может скрываться мошенническая махинация.

Обычно работа связана с переводом денег или обналичиванием средств. Не стоит забывать поговорку «бесплатный сыр бывает только в мышеловке». Поэтому ни в коем случае не откликайтесь на такие вакансии, если не хотите оказаться соучастником преступления.

Если вам понадобится кредит, то для оформления пользуйтесь только официальными инструментами — приложениями и сайтами банков. Как, например, этот сайт. Ниже в форме посчитайте комфортные условия и отправляйте заявку в банк.

Дропперы, или дропы, — что это за люди

Дроппер – это человек, которого используют мошенники для достижения своих целей. Он не является инициатором преступления, а выполняет указания, получая за это деньги.

Дропы участвуют во всех схемах по обналу (незаконное обналичивание) чужих денег. Схема довольна проста: дроппер предоставляет данные своей банковской карты, на которую переводят средства, добытые преступными способами. Затем он обналичивает сумму в банкомате, передает другим лицам и получает определенный процент со сделки.

Казалось бы, зачем усложнять работу и нанимать подставных людей? К услугам дропов обращаются, во-первых, чтобы самому мошеннику не засветиться и не получить наказание. Во-вторых, чтобы скрыть сам факт киберпреступления и сделать цепочку переводов более запутанной, ведь операции проводятся под разными именами.

Никому не сообщайте данные вашей карточки

Иногда люди осознанно соглашаются на такую работу, но в других случаях компания может так шифроваться, что вы и не узнаете, что вовлечены в нелегальные схемы. Так что внимательно изучайте условия, ведь у предложений работать дроппером есть некоторые отличительные особенности:

- рассматриваются соискатели без какого-либо образования, опыта;
- работа связана с переводом либо обналичиванием денег;
- полная удаленная занятость, нет необходимости явиться в офис для оформления документов;
- неофициально;
- не указана хотя бы примерная зарплата;
- либо предлагают сразу много денег буквально за несколько часов работы.

Как используют дропов

Существует много схем для получения незаконного заработка. Перевод с одной пластиковой карточки на другую и затем снятие средств в банкомате – это, пожалуй, самый наглядный пример работы дропов и один из вариантов использования их труда.

Наверняка вам хотя бы один раз звонили и представились сотрудниками определенной банковской организации. Обычно они сообщают, что злоумышленники пытались списать средства со счета либо уже это сделали, а чтобы защитить ваши деньги, необходимо передать «сотрудникам» личные данные.

Если вы сообщите эту информацию, то мошенникам не составит труда украсть деньги с вашего счета.

Это один из способов черного заработка. Для звонков нанимают специальных людей (дропперов), а переводами, например, может заниматься другая группа.

Другой пример интернет-мошенничества – продажа товара по предоплате. Обычно это интернет-магазины, которые на первый взгляд кажутся официальными: реклама, все подтверждающие документы, отзывы от покупателей. Они регистрируются как ООО, а генеральным директором делают дропа.

Схема выманивания денег у лжепродавцов такова: они просят предоплату за товар, люди им отправляют деньги, но взамен не получают желанной покупки. Через некоторое время такие онлайн-платформы закрываются, и вернуть свои средства не получится.

Выяснить, кто являлся организатором дела, почти невозможно, а подставным лицом мог стать любой человек, даже сам того не подозревая.

Существует понятие «разводной дроппер», чьи конфиденциальные данные злоумышленники получают обманным методом. Например, они размещают вакансию курьера. Если кто-то откликается на нее, то его просят отправить сканы документов, обычно паспорт со СНИЛС, чтобы «пройти проверку службы безопасности».

Человеку не перезванивают насчет работы, а его данные мошенники могут использовать для любых целей.

Что вынуждает людей становиться дропами

Основные причины – отсутствие денег, нестабильное финансовое положение. Также могут влиять такие субъективные факторы, как желание получить легкие деньги, быстро разбогатеть. Дропперы в среднем получают до 40% от сделки, а это больше, чем среднестатистическая заработная плата в стране.

Чаще всего осознанно сотрудничать с мошенниками начинают безработные и люди из низшего слоя общества. Такими людьми легко

управлять и манипулировать. Обычно на таких дропперов оформляют займы, подставные фирмы.

Независимо от того, что людей подтолкнуло к такому занятию, оно уголовно наказывается

Кто еще становится дропами:

- студенты;
- мигранты из деревень, маленьких городов;
- иммигранты из других стран, обычно экономически не развитых;
- другие уязвимые слои населения (сироты, многодетные семьи, безработные).