Как снять жилье и не попасть на мошенников

В области участились случаи мошенничества со сдачей квартир в аренду. При этом мошенники используют популярные торговые площадки, в достоверности которых граждане не сомневаются.

Цена за такие жилища, как правило, значительно меньше аналогичных предложений, что, несомненно, вызывает интерес у будущих квартиросъемщиков.

Следует отметить: для того, чтобы войти в доверие к потерпевшим, злоумышленники в переписке сбрасывают фотографию паспорта, рассказывают о ажиотаже на данную квартиру, просят внести предоплату, которая гарантировала бы бронирование жилья.

Кроме того, зачастую с гражданином, который перевел задаток, связывается якобы арендодатель и под различными предлогами указывает на причину невозможности заселения лица в съемную квартиру (она занята, сломан ключ от входной двери и т. д.), при этом для возврата денежных средств потенциальному квартиросъемщику отправляет в мессенджер фишинговую ссылку, перейдя по которой и внеся данные своей банковской платежной карты, человек лишается денежных средств, имеющихся на счету.

Если вы желаете снять в наем квартиру, необходимо связываться с хозяином или сотрудником агентства не только посредством интернет мессенджеров. Не стоит жалеть своего времени: следует договориться о личной встрече, в результате которой можно осмотреть квартиру, составить необходимые документы. Если нет возможности лично проверить жилье - попросите об этом своих знакомых. Необходимо обращать внимание на номера телефонов и счета, которые указывают на объявления (они должны быть оформлены в белорусских сотовых компаниях и банках). Также важно требовать документы, подтверждающие принадлежность квартиры арендодателю (свидетельства, доверенности).

Как купить морепродукты через интернет и не лишиться денег

Основным видом регистрируемых киберпреступлений являются интернет-мошенничества. На сегодняшний день широко распространен такой вид преступной деятельности, как обман, совершаемый в соцсетях с использованием мошеннических интернет-магазинов под предлогом купли-продажи морепродуктов. Как правило, стоимость таких «морепродуктов» гораздо ниже рыночной. Добросовестный покупатель вносит предоплату или оплачивает полностью приобретенный товар и, в итоге, остается и без денег, и без покупки.

Приведем несколько последних примеров данного вида мошенничества, зарегистрированных на территории Могилевской области.

Так, бобруйчанин, 1992 г.р., обратился в милицию с заявлением. Он пояснил, что 26 апреля неизвестный с использованием глобальной сети

Интернет в мессенджере «Telegram» на одном из сайтов обманным путем под предлогом продажи морепродуктов завладел 150 рублями, переведенными на карт-счет ОАО «Сбербанк».

Через пару дней обманута мошенниками была еще одна любительница морепродуктов из того же города. С женщиной, 1988 г.г., в социальной сети «Instagram» также связался незнакомец и попросил оплатить товар: гражданка в итоге осталась без продукции и 270 рублей.

А могилевчанка, 1975 г.р., через аккаунт в мессенджере «Telegram» также хотела приобрести морскую рыбу и была обманута: думая, что расплачивается за товар, перевела на банковский счет мошенников 130 рублей.

Во всех случаях следователями возбуждены уголовные дела по фактам мошенничества.

Чтобы не стать жертвой киберпреступников, рекомендуем пользоваться только официальными сайтами и не переходить (в том числе по ссылкам) на сомнительные площадки. Перед покупкой товаров в интернет-магазинах необходимо обратить внимание на наличие на странице номера телефона для того, чтобы «в живую» пообщаться с продавцом и уточнить все интересующие вопросы по заказу. Мошенник вряд ли на странице укажет номер телефона, а если и оставит, то не будет выходить на связь.

Кроме того, не стоит доверять продавцу, требующему внести предоплату за покупку или услугу.

О покупке аккаунтов в онлайн-играх

В настоящее время онлайн-игры стали уже не только развлечением, но и своеобразным активом: за долгую игровую жизнь персонажи обрастают достижениями, уникальными вещами, бонусами. Все это может быть похищено или разрушено, если геймер не заботится о защите своего аккаунта.

Важные советы любителям онлайн-игр:

- создайте сложный пароль (буквы разного регистра, специальные символы) и регулярно меняйте его. Если пароль все-таки утечет в сеть, то регулярное изменение даже одной цифры или буквы поможет спасти аккаунт. При этом к старым комбинациям лучше не возвращаться;
- отключите функцию «сохранить пароль» при входе в свой профиль на чужих устройствах. А когда закончите играть, проверьте, точно ли вы вышли из аккаунта.

В каждой виртуальной вселенной есть возможность ее улучшения - нужно только привязать карту и оплатить апгрейд. Не стоит забывать о том, что в первую очередь необходимо делать покупки только через официальные платформы (Steam, PlayStation Store, App Store), а также не переходить по ссылкам с других сайтов, где предлагают «скины» по низкой цене или вовсе бесплатно.

Не привязывайте к игре зарплатную карту, это может привести к нежелательным последствиям. Если платформа имеет слабую систему защиты, то данные карты (а значит, и деньги) могут попасть к злоумышленникам. А еще многие игры предлагают внутриигровые покупки, подписки и бонусы, средства за которые могут списываться автоматически (по подписке). Поэтому для онлайн-покупок следует завести отдельную (можно виртуальную) карту с ограниченным балансом, установить на ней лимит и зачислять не нее только ту сумму, которую вы готовы потратить на игры.

Пользование чужой банковской картой - это преступление, хищение имущества путем модификации компьютерной информации (статья 212 УК Республики Беларусь).

Так, недавно уголовное дело было возбуждено в отношении девятиклассника, который привязал к игре банковскую карточку бабушкиной подруги. Женщина, находясь в гостях, оставила сумку с кошельком без присмотра. Мальчик незаметно переписал номер и CVV-код БПК, после чего с помощью нее рассчитался за бонусы в виртуальном мире, списав вполне реальные 2 400 рублей.

9-летняя ученица по указанию незнакомца, пытаясь купить аккаунт, продиктовала доступ к личным данным матери, воспользовавшись ее сотовым телефоном. С банковской карты списана немалая сумма денег.

УВД Могилевского облисполкома рекомендует родителям доступным языком объяснять ребенку правила поведения и безопасности, в том числе в виртуальной среде. Необходимо разъяснить им, что ни в коем случае нельзя передавать данные банковских карт и иную личную информацию третьим лицам. Правила финансовой грамотности стоит обсуждать с несовершеннолетними уже с раннего возраста.

Сезонные товары: будьте бдительны при их покупке через интернет

На сегодняшний день широко распространен такой вид преступной деятельности, как обман, совершаемый в социальных сетях с использованием мошеннических интернет-магазинов под предлогом продажи садовой мебели, в том числе качелей.

По словам заместителя начальника УВД Могилевского облисполкома - начальника криминальной милиции Евгения Бутько, стоимость указанных товаров у таких продавцов гораздо ниже рыночной. Зачастую покупатель вносит предоплату либо оплачивает полностью приобретаемый товар, но остается без денег и без покупки.

Сейчас лето и особым спросом пользуются сезонные товары, среди которых и садовые товары. При их покупке через интернет граждане продолжают попадаться на уловки мошенников, а после обращаются за помощью к правоохранителям Могилевщины.

Вот несколько последних случаев.

Бобруйчанка, 1981 г.р., сообщила в милицию о том, что в мае неизвестный с использованием глобальной сети Интернет в социальной сети «Инстаграмм» через приложение М-банкинг с карт-счета под предлогом продажи садовой качели завладел ее деньгами в сумме 550 рублей, которые заявительница перевела на карт-счет указанного банка.

На такую же уловку попала и жительница Горок, 1989 г.р., у которой аналогичным путем были похищены 590 рублей.

В милицию с заявлением обратился и могилевчанин, 1985 г.р. Желая купить мебель для сада, он перевел на банковскую карту незнакомца 650 рублей.

В начале июня 700 рублей подобным образом лишилась жительница агрогородка Бацевичи, 1987 г.р. Теперь женщина и без качелей, и без денег.

По всем указанным фактам следователями возбуждены уголовные дела.

Чтобы не стать, жертвой мошенников, покупая садовую мебель и прочие товары, важно быть бдительным и не поддаваться на сомнительные предложения. Перед приобретением товаров в интернет- магазинах необходимо обратить внимание на наличие на странице номера телефона, для того чтобы «в живую» пообщаться с продавцом и уточнить все интересующие вопросы по заказу. Также не стоит вносить предоплату за покупку или услугу.

Как защитить себя от кибермошенничества

Кибермошенники постоянно совершенствуют методы обмана, используя новые технологии и социальную инженерию, поэтому необходимо быть в курсе актуальных схем. Ниже представлены наиболее распространенные сценарии мошенничеств и рекомендации по профилактике.

- ***Совершение мошеннических действий под видом работников коммунальных служб и государственных органов.***

Злоумышленники выдают себя за сотрудников коммунальных служб (энергонадзора, водоканала, газовой службы), а также представителей правоохранительных органов, банков или других государственных структур. Они могут звонить по телефону, в том числе по стационарной линии, или использовать мессенджеры (Viber, Telegram, WhatsApp). Цель - под любым предлогом получить личные данные, реквизиты банковских карт или вынудить перевести деньги на «безопасные» счета. Macro работают в паре: один представляется сотрудником коммунальной службы, другой - правоохранительных органов или банка, убеждая жертву, что ее данные скомпрометированы и для «спасения» средств необходимо оформить кредит или перевести деньги.

Приведем примеры подобных преступлений, имевших место на территории Могилевщины.

Пенсионерка из Горок, 1944 г.р., заявила в милицию о том, что 19 июня неизвестный с использованием глобальной сети «Интернет» в мессенджере «Viber», представившись сотрудником Департамента финансовых расследований, под предлогом декларирования денежных средств, убедил установить приложение удаленного доступа мобильного оператора, после чего с ее банковского счета похитил 7500 рублей.

Жителю агрогородка Новые Самотевичи, 1958 г.р., в мессенджере «WhatsApp» также позвонил неизвестный и, представившись сотрудником правоохранительных органов, обманным путем, под предлогом сохранности денежных средств, похитил с его банковской карты 11900 рублей.

Мошенничества с использованием мобильной связи

Злоумышленники представляются сотрудниками операторов сотовой связи (A1, МТС). Под предлогом окончания срока действия договора или необходимости обновления услуг они убеждают жертву перейти по ссылке из мессенджера и скачать поддельное приложение. Последнее дает злоумышленникам полный доступ к данным на смартфоне, включая коды из SMS, логины и пароли к онлайн-банкингу.

и

Важно помнить: безопасное скачивание приложений возможно только из официальных магазинов, таких как Google Play, App Store, App Gallery. Никогда не устанавливайте приложения, переходя по сомнительным ссылкам.

С пенсионеркой из Могилева, 1949 г.р., неизвестный связался посредством мессенджера «WhatsApp». Представился сотрудником одной из мобильных кампаний и под предлогом продления договора об оказании услуг, посредством неустановленной фишинговой ссылки программного обеспечения мобильного оператора, с карт-счета женщины похитил 6000 рублей.

Жительница агрогородка Махово Могилевского района, 1949 г.р., также попала на уловку мошенника. В июне неизвестный с использованием глобальной сети «Интернет» в мессенджерах «Viber» и «WhatsApp» позвонил пенсионерке и, представившись сотрудником мобильного оператора и правоохранительных органов, под предлогом смены тарифного плана и продления договора об оказании услуг, убедил сообщить реквизиты ее банковской карты и коды, приходящие по СМС. После этого с указанного карт-счега похитил более 2600 рублей.

Во всех перечисленных случаях следователями возбуждены уголовные дела.

Деньги на карте: как защитить сбережения

Онлайн-платежи неотъемлемая часть нашей жизни: такси, оплата ЖКУ, маркетплейсы — всё это быстро и удобно. Но есть и обратная сторона медали: крупная сумма на обычной дебетовой карте делает гражданина приоритетной мишенью для киберпреступников.

Даже осторожные пользователи могут вовремя не распознать фишинговый ресурс или поддаться приемам социальной инженерии.

Как обезопасить свои деньги? Несколько практичных правил

Держите на карте "оперативный минимум". Используйте дебетовую карту только для текущих расходов.

Пользуйтесь виртуальными картами. Создавайте их специально для конкретных операций или на короткий срок (в большинстве банковских приложений это можно сделать за пару минут). Даже если данные утекут, основная карта и ваши сбережения останутся в безопасности.

Ограничьте суммы на снятие наличных и оплату покупок. Это сдержит мошенников, даже если они завладеют данными карты. А мгновенные push-уведомления о любых операциях помогут вовремя среагировать на подозрительный платеж.

Заведите отдельную карту/счет исключительно для подключенных автоплатежей (ЖКУ, подписки). Пополняйте его только на нужную сумму. Это изолирует ваши основные средства и автоплатежи от риска (а также поможет их оценить и контролировать).

Узнайте, как мгновенно заблокировать карту через мобильное приложение банка (не только по звонку). Это критично, если телефон утерян или вы заметили подозрительную операцию.

Помните: осознанное управление деньгами и разумные меры предосторожности сводят шансы мошенников к минимуму.

Будьте бдительны: интернет-мошенники через детей получаю! доступ к сбережениям взрослых

В последнее время на территории соседнего государства участились мошеннические звонки подросткам от имени якобы школьных и университетских психологов с целью получить конфиденциальную информацию о сбережениях их родителей. В целях профилактики расскажем об этой схеме.

Под предлогом необходимости пройти «психологическое тестирование» или «проверить данные» злоумышленники присылают фишинговую ссылку в мессенджеры, затем запугивают подростков, утверждая, что их личные данные «утекли» в сеть и грозят уголовным преследованием.

Затем мошенники «переключают» жертву на лжесотрудников правоохранительных органов, которые могут проводить видеозвонки, находясь в форменном обмундировании, показывать поддельные

удостоверения и требовать полной секретности («Ничего не рассказывай родителям!»)

Используя психологические приемы, подростков убеждают:

- тайно снимать и переводить крупные суммы денег со счетов родителей;
- оформлять кредиты на себя или родителей;
- передавать наличные курьерам (иод разными предлогами: «для сохранности», «на экспертизу», «в залог»).

Гак, в одном из зарегистрированных на территории соседнего государства случаев мошенники, действуя под видом вымышленных психолога и следователя, убедили студентку в течение недели тайно снять и перевести крупную сумму со счета отца и в дальнейшем оформить кредит.

Правоохранители обращают внимание на то, что подобные мошеннические схемы могут быть реализованы и на территории Республики Беларусь. Поэтому проведите соответствующую разъяснительную беседу со своими детьми, рассказав о новых преступных схемах в интернете. В целях профилактики сведения о своих банковских картах и счетах держи те в конфиденциальности.

Рекомендации по безопасному использованию мессенджеров

Общаясь в мессенджерах важно оценивать безопасность и риски, связанные с их использованием. Необходимо соблюдать определенные правила общения в соцсетях, не забывая о том, что злоумышленники используют современные способы и методы, чтобы охотиться за вашими деньгами и личными данными.

-Скачивайте приложения мессенджеров только с сайтов разработчиков и официальных магазинов приложений.

- Настройте двухфакторную аутентификацию в приложении мессенджера.
- Запретите в настройках получение сообщений от незнакомых контактов.
- Отключите автозагрузку файлов.
- С подозрением относитесь к полученным ссылкам и файлам, даже если они поступили от известного отправителя. Прежде чем переходить по ссылке или открывать файл, узнайте другим способом связи, действительно ли ваш знакомый отправлял их.
- Отключите функцию, позволяющую просматривать ваш профиль всем пользователям (сделайте его доступным только для ваших контактов).
- Избегайте обмена конфиденциальной информацией в чатах.
-Соблюдайте осторожность при использовании мессенджеров через общедоступные сети Wi-Fi.
- Регулярно обновляйте все установленные программы и операционную систему своих устройств.

Новая схема обмана в сети: как ее распознать и что делать?

В последнее время участились случаи, когда мошенники представляются сотрудниками мобильного оператора «МТС». Под выдуманными предлогами (необходимость продления договора, страхование или декларирование денежных средств) они предлагают установить приложение удаленного доступа «Мой МТС.арк», а получив доступ к мобильному устройству похищают с карт-счета сбережения доверчивых граждан.

Запомните: установив фейковое приложение, вы тем самым даете мошенникам доступ к своим данным, включая логины и пароли. Это позволяет преступникам свободно получать информацию о банковских счетах, личной переписке и других конфиденциальных сведениях!

Так, пенсионерка из Круглого, установив приложение «Мой МТС», после общения с лже-оператором сотовой сети, лишилась более 1 000 рублей, а жительница Кричева, спасая свои сбережения, пополнила банковский счет и сообщила мошенника логин и пароль от М-банкинга, потеряв около 15 000 рублей.

Чтобы не стать жертвой киберзлоумышленников следуйте простым правилам:

- сотрудники мобильных операторов не звонят абонентам через мессенджеры и не используют номера иностранных операторов, а также никогда не требуют изменить пароли под диктовку;

-договоры с компанией МТС заключаются на бессрочной основе и продлеваются автоматически;

-если вы получаете звонок через любой мессенджер с неизвестного номера, не передавайте личные данные, прервите разговор и обратитесь в официальный контактный центр МТС (0890) для проверки информации;

- приложение «Мой МТС» можно скачать только из официальных магазинов Google Play. App Store и App Gallery;

никогда не устанавливайте приложение по ссылкам, полученным от неизвестных источников через мессенджеры ил присланные в виде АРК-файла.

Будьте бдительны: как распознать лжеоператора сотовой связи в собеседники?

Доверчивые граждане продолжают попадать на уловки мошенников, которые под видом операторов сотовой связи втираются к ним в доверие и используют их личные данные (идентификационные сведения, реквизиты банковских платежных карт, СМС-коды) в своих корыстных целях.

Существует множество сценариев, следуя которым злоумышленники вводят в заблуждение своих потенциальных жертв. Вот несколько из них:

После общения с незнакомцами, представившимися оператором «МТС» и правоохранителем, могилевчанин чуть было не лишился 3000 рублей, в то время как жителя Горок лжесотрудник сотовой связи обманным путем убедил оформить кредит на сумму около 30 000 рублей, которыми пытался завладеть.

Жительница областного центра и не предполагала, что приятный собеседник, с которым она общается - мошенник. Под предлогом продления срока договора об оказании услуг с ее банковской карты было похищено около 4000рублей. На такую же уловку попалась и бобруйчанка. Сообщив лжеоператору свои паспортные данные и СМС-коды, с ее карт- счета были списаны около 1000рублей.

Сотрудники милиции напоминают: чтобы защитить себя от мошенников будьте бдительны и следуйте простым правилам:

- сотрудники мобильных операторов не звонят абонентам через мессенджеры и не используют номера иностранных операторов. Они никогда не требуют изменить пароли под диктовку;
- в случае если вас переадресовали на звонок от лица, который представился сотрудником государственных органов, необходимо уточнить его должность, специальное звание и подразделение. После чего осуществить звонок по номеру «102» и уточнить, работает ли такой сотрудник в правоохранительных органах;
- договоры с компанией «МТС» заключаются на бессрочной основе и продлеваются автоматически;
- если вы получаете звонок через любой мессенджер с неизвестного номера и лицо представилось сотрудником оператора сотовой связи, не передавайте личные данные, прервите разговор и обратитесь в официальный контактный центр оператора сотовой связи для проверки информации.

Мошенники и код от домофона: как работает новая схема обмана

Мошенники начали обманывать граждан, используя новый предлог. Аферисты звонят и, представляясь сотрудниками компаний по установке домофонов, предлагают бесплатную замену ключей. Под видом «плановой замены чипов» запрашивают личные данные человека. Если «клиент» соглашается, то следом они запрашивают код из SMS, который направляется якобы «от компании» и будет использован для открытия домофонной двери.

Позже с другого номера поступает звонок от лжеправоохранителя, который сообщает о попытке взлома системы и под предлогом предотвращения мошеннических действий, убеждает гражданина сообщить ФИО, дату рождения, реквизиты банковских карт, коды из SMS и пин-коды.

Получая доступ к личным данным (аккаунтам, кабинетам) жертвы, злоумышленники имеют возможность совершать от ее имени различные действия: оформлять кредиты (доверенности), похищать денежные средства с банковских счетов и т.п.

Так, на уловку таких мошенников уже попали жительницы областного центра и Бобруйска, которые перевели злоумышленникам более 5000 рублей.

Как не потерять свои сбережения:

- никогда не сообщать одноразовые SMS-коды посторонним;
- помнить, что сотрудники правоохранительных органов, банковских и иных учреждений не связываются с гражданами по мессенджерам;
- незамедлительно прекращать разговор с незнакомцем;
- обращаться к представителям банков, в государственные органы и учреждения только через официальные сайты и контактные телефоны, размещенные на них;
- не переходить по подозрительным ссылкам и не скачивать приложения из неизвестных источников.

Если незнакомцы по телефону требуют от вас совершить какие-либо манипуляции с финансами (задекларировать, положить на безопасный счет и т.д.) - немедленно прекратите разговор и сообщите об этом в милицию!

Киберпреступность в молодежной среде: факторы риска и ответственность

Современные подростки значительную часть своего свободного времени проводят в виртуальном пространстве. Однако возможности Всемирной паутины можно использовать по-разному, в том числе и в преступных целях.

Проблематика подростковой преступности - одной из самых существенных проблем общества. Многие забывают, что ответственность (как уголовная, так и административная) за совершение киберпреступлений наступает с 16 лет, а за некоторые деяния уже с 14 лет. Таким образом, иногда просто шутка или на первый взгляд безобидное действие, могут повлечь за собой серьезные последствия!

Одним из самых распространенных противоправных проступков, которые совершают несовершеннолетние в виртуальном пространстве (в том числе при их соучастии) считается **мошенничество** (статья 209 УК Республики Беларусь) и **хищения имущества путем модификации компьютерной информации** (статья 212 УК Республики Беларусь).

Так, несовершеннолетний могилевчанин, представившись девушкой, начал переписку с жителем областного центра в одном из мессенджеров. Войдя в доверие к собеседнику путем обмана выманил у последнего около 2000 рублей, которые доверчивый мужчина перевел на предоставленные мошенником банковские счета.

На уловку мошенника-подростка из Кличева попали 3 могилевчан, которые перевели мошеннику около 1000рублей.

Зачастую подростки совершают противоправные действия с целью самоутверждения или ищут в сети Интернет способы легкого заработка. Однако и не подозревают, кто может скрываться за обликом «желающих помочь заработать» и склоняют детей к совершению преступлений и правонарушений.

Следует помнить, что за **незаконный оборот платежных инструментов, средств платежа и их реквизитов (статья 222 УК** Республики Беларусь), **заведомо ложные сообщение об опасности** (статья 340 УК Республики Беларусь) **и незаконное предоставление реквизитов платежных инструментов** (статья 12.35 **КоАП** Республики Беларусь), также предусмотрена ответственность.

Несовершеннолетний бобруйчанин неоднократно звонил с разных абонентских номеров на телефоны оперативно-дежурных служб правоохранительных органов Бобруйска и сообщал заведомо ложные сведения о готовящихся взрывах на территории города

Жажда легкого заработка обернулась для подростка из Черикова административной ответственностью. Молодой человек незаконно продал свои аккаунт и личные данные третьим лицам, как позже выяснилось мошенникам. Получив доступ к счетам (электронным кошелькам) злоумышленники с их помощью стали обманывать добропорядочных граждан.

В последнее время наблюдается повышенный интерес к сделкам с криптовалютой. Однако многие забывают, что физические лица могут осуществлять операции с криптой исключительно в собственных целях! Любое посредничество со стороны третьих лиц - незаконно!

Соблюдайте простые правила и рекомендации для безопасного использования Интернета:

для детей 10-13 лет:

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета;
- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;

На данном этапе могут активно использоваться программные средства родительского контроля, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;
- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);

Для подростков 14-17 лет:

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;

настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета;

- напоминайте о необходимости обеспечения конфиденциальности личной информации;
- предостерегайте детей от использования сети для совершения противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей родители должны незамедлительно сообщать о них классному руководителю в школе, социальному педагогу учреждения образования и обратится в территориальный отдел внутренних дел по месту жительства.

Новая схема обмана: как мошенники обманывают граждан под видом «Белпочты»

В последнее время участились случаи, когда злоумышленники действуют от имени представителей почтовых отделений. Схема проста: они рассылают sms-сообщения с фишинговыми ссылками, утверждая, что доставка посылки невозможна ввиду отсутствия адреса. Потенциальной жертве предлагают перейти на «официальный сайт», ввести свои персональные данные и оплатить повторную отправку посылки.

Также мошенники регистрируют личные кабинеты на портале «Белпочты». После чего связываются с гражданами посредством мессенджеров и пытаются узнать код подтверждения из сообщения, чтобы далее действовать от их имени.

Так, 54-летняя могилевчанка, желая получить письмо, лишилась более 2000 рублей, списанных с ее карт-счета. В то же время 56-летней жительнице областного центра повторное оформление доставки посылки обошлось более чем в 19000 рублей, перечисленных злоумышленникам с ее банковской карты.

Помните: коды из sms-сообщений - это конфиденциальная информация, которую нельзя сообщать третьим лицам. Если вы стали жертвой подобной схемы обмана, незамедлительно смените пароль на портале «Белпочты» или в мобильном приложении организации и сообщите по номеру «102».

Сотрудники почтовых отделений информирует о прибытии отправлений, но никогда не требует онлайн-оплаты услуг через

сомнительные ссылки и ввод данных банковских карт. Проявляйте осторожность при переходе в интернете и всегда проверяйте адрес сайта.

Поддельные письма от ГАИ: еще один способ мошенничества

Злоумышленники придумывают все новые уловки, чтобы завладеть чужими деньгами. Граждане по электронной почте или в мессенджере получают сообщение с формулировкой: «Вы нарушили ПДД. Ознакомьтесь с постановлением и оплатите штраф до 01.10». К письму прикреплён файл в формате PDF, оформленный под официальное постановление. В документе может быть указано реальное имя человека, номер автомобиля или иные персональные данные - это создаёт ощущение подлинности.

В самом письме размещена кнопка «оплатить сейчас», ведущая на стороннюю интернет-страницу. Переход по ссылке приводит к различным вариантам развития событий.

В некоторых случаях пользователь попадает на фальшивый сайт, визуально копирующий интерфейс государственных или банковских онлайн-сервисов. Здесь у него запрашивают данные банковской карты: номер, срок действия, CVV-код, а иногда и коды подтверждения из СМС. Иногда ссылка ведёт на заражённый ресурс, который автоматически загружает вредоносное программное обеспечение на устройство пользователя. Такое ПО может перехватывать пароли, получать доступ к банковским приложениям, мессенджерам и даже использовать камеру и микрофон.

Зачастую новые схемы обмана, «обкатываемые» мошенниками в соседних странах, в последующем используются и в Республике Беларусь И хоть на Могилевщине на подобные уловки мошенников граждане пока не попадались, в целях профилактики напомним о безопасности. «Письма счастья» в нашей стране автовладельцу направляются заказным письмом через РУП «Белпочта», на мобильный телефон поступает соответствующее смс-уведомлсние. Для оплаты штрафа в ЕТИП необходимо сверять все имеющиеся реквизиты и только после этого приступать к переводу денег.

Вам звонят: кибермошенники теперь представляются и сотрудниками отдела по образованию

В сопредельных государствах злоумышленники мспользуют нову, но очень простую и убедительную преступную схему выманивания денег у граждан.

Незнакомые абоненты звонят людям от имени бухгалтера отдела по образованию района и сообщают о положенной выплате или необходимости оформить документы лично в администрации. Называют время записи, номер кабинета и поясняют, что дистанционно это сделать нельзя. В конце разговора, как бы спохватившись, просят продиктовать паспортные данные якобы для оформления временного пропуска. Всё выглядит настолько официально, что усомниться трудно

Чаще всего в первом этапе злоумышленники выманивают код авторизации из SMS или одноразовый пароль - именно с их помощью реально полупить доступ к значимым аккаунтам. Паспортные данные сами по себе для взлома недостаточны, однако нужны для создания психологического эффекта.

Дальше следует стандартный сценарий: к беседе подключаются «представители правоохранительных органов» или «специалисты по безопасности», сообщая о якобы обнаруженной утечки данных, «финансировании террористов» или других тяжких обстоятельствах, наступивших из-за того, что паспортные данные попали в руки мошенников.

Почему это работает: официальный язык, конкретика (номер кабинета, должность), перечисление бюрократических процедур снижает бдительность — человек воспринимает просьбу звонящего рутинную служебную формальность.

Выявить, когда начала работать мошенническая схема в таких ситуациях довольно сложно. Поэтому чтобы обезопасить себя, даже совершенно безобидные, на первый взгляд, приглашения стоит проверять, используя официальные каналы связи.