Новая уловка: теперь мошенники представляются работниками энергосбыта

В последнее время в области участились случаи, когда мошенники звонят гражданам и представляются сотрудниками «Энергосбыта». Злоумышленники связываются с жертвами и заявляют о необходимости замены электрических счетчиков, для чего запрашивают их персональные данные. Далее мошенники переходят ко второму этапу. Потерпевшему в мессенджер звонят якобы представители правоохранительных органов или банка и убеждают жертву «задекларировать» свои денежные средства, переведя их на так называемый «безопасный счет», либо оформить кредит.

Так, 60-летней жительнице одного из районных центров Могилевщины в мессенджере позвонил неизвестный, который представился работником «Энергосбыта». В ходе разговора собеседник сообщил, что электрические счетчики пенсионерки подлежат замене и ей необходимо предоставить паспортные данные для регистрации, что она и сделала. Позже с женщиной связались якобы представители банка. Они убедили пенсионерку оформить заявку на получение кредита на сумму более 11 000 белорусских рублей. Однако лжебанкирам не удалось довести преступный умысел до конца, так как гражданка поняла, что общается с мошенниками, в результате чего аннулировала заявку на получение кредита.

Запомните! Если вам звонят незнакомцы в мессенджере и утверждают, что являются представителями правоохранительных органов или государственных учреждений, просят сообщить ваши личные данные и предлагают перевести деньги на «безопасные счета» – это мошенники! Сотрудники правоохранительных органов и других государственных служб не используют для связи с гражданами мессенджеры либо соцсети, не направляют абонентам ссылки для решения вопросов, не требуют осуществления финансовых операций! При поступлении подобных звонков необходимо немедленно прекратить разговор и сообщить о случившемся в милицию!

По материалам УПК УВД Могилевского облисполкома

Будьте бдительны: интернет-мошенники через детей получают 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 (под разными предлогами: «для сохранности», «на экспертизу», «в залог»).

Так, 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 держите в конфиденциальности.

Управление по противодействию киберпреступности КМ УВД

Опасности, с которыми может столкнуться ребенок в сети

Риски, с которыми ребенок может столкнуться в интернете, можно разделить на четыре категории.

- Контентные – это тексты, фото, видео, демонстрирующие насилие, порнографию, пропаганду нездорового поведения.
- Коммуникационные – сомнительные знакомства, буллинг (травля), груминг (дружба с целью эксплуатации), шантаж, сексуальные домогательства.
- Потребительские и технические риски – в обоих случаях ребенок может столкнуться с хищением персональных данных (например, паролей от соцсетей) или контента со своего компьютера, планшета или смартфона.

Как ни странно, но статистика поисковых запросов доказывает, что родители ошибаются, определяя сексуальный контент как главную угрозу для ребенка в сети. Дети куда чаще ищут, как сделать слайм или признаться в любви. С одной стороны, это хорошие новости, но с другой – важно, чтобы родители знали сами и предупреждали детей о куда более широком спектре опасностей, которые могут подстерегать их в интернете. А еще умели выстраивать защиту ребенка так, чтобы он не стремился из-под нее вырваться. Сделать это можно, соблюдая несколько простых правил.

Какие онлайн-правила поведения должны быть в семье?

Первое: не запрещайте

Часто родителям кажется, что запрет на использование гаджета – лучший способ решить проблему. Но у такой стратегии есть два больших минуса: запреты нарушают доверительные отношения между родителями и ребенком («не буду им ничего говорить, а то еще телефон отнимут») и ничему не учат. Киберграмотности надо обучать так же, как и правилам безопасности на дороге или обращению с деньгами: сначала теория, потом практика под наблюдением родителя, а затем самостоятельное применение правил.

Второе: пользуйтесь программами родительского контроля

Программы для детской онлайн-безопасности помогают родителям сопровождать ребенка, пока он делает свои первые шаги в сети. С помощью этих установок родители могут оградить ребенка от нежелательного контента, вовремя понять, что он столкнулся

не фотографируете ценные вещи дома, не размещаете посты, на которых видны детский сад или школа вашего ребенка.

Пятое: не ругайте за любопытство

Детям всегда был интересен «взрослый» мир, задолго до появления интернета. Главная причина этого – любопытство. У ребенка есть вопросы, и сейчас чаще всего он ищет ответы на них в интернете. Задача родителей – понять, почему у чада появился интерес, и быть готовым поговоритьс ним об этом. Не обвинять, не ругать, а поинтересоваться: «А как ты об этом узнал? А что еще ты знаешь об этом? Давай разберемся, почему информация, которая у тебя есть сейчас, не совсем верна». И не спешите доставать с полки энциклопедию 50-х годов – можно воспользоваться тем же интернетом, ведь современный ребенок гаджету доверяет куда больше.

По материалам УПК УВД Могилевского облисполкома

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.

Не стать жертвой телефонных мошенников

Мошенники под видом работников банка, операторов связи или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении (вишинг). При этом чтобы войти в доверие, могут выслать фото служебных документов или даже выйти по видеосвязи в мессенджере.

Распространен способ, когда злоумышленники, используя различные вымышленные ситуации, убеждают потенциальных жертв загрузить направленный в мессенджере файл или установить определенное мобильное приложение. В обоих случаях мошенники получают возможность удаленно управлять устройством, на котором оно установлено. Таким образом, получают доступ к личным данным пользователей, в том числе имеют возможность оформить онлайн-кредит. Также злоумышленники убеждают оформить кредиты в банках, а деньги перевести на «защищенный» счет.

Вот несколько свежих фабул подобных преступлений.

Пенсионерке из Могилева, 1942 г.р., в мессенджере «Viber» с неизвестного номера позвонил мужчина, который представился сотрудником финансовой милиции. После посредством приложения удаленного доступа «Webkey DashBoard» с ее банковской карты пытался похитить 5500 рублей.

Аналогичным способом была обманута и бобруйчанка, 1952 г.р.: с использованием того же мессенджера ей позвонил якобы сотрудник правоохранительных органов. Под предлогом декларирования и сохранения денежных средств, обманным путем он завладел 5000 рублями, которые были переведены с банковской карты женщины.

Еще одного пенсионера, 1942 г.р., проживающего в областном центре, также обманул неизвестный, но уже с использованием мессенджера «WhatsApp». Он представился сотрудником одного из операторов сотовой связи, под предлогом продления договора, убедил пожилого человека, установить приложение удаленного доступа, после чего с банковской карты пенсионера похитил 4300 рублей.

Во всех указанных случаях возбуждены уголовные дела.

Чтобы не попасть на уловки телефонных мошенников, важно соблюдать правила безопасности:

- всегда надо быть начеку и не доверять незнакомым,
- ни под каким предлогом не устанавливать непроверенные программы и файлы, полученные в мессенджере от неизвестных,
- не передавать кому бы то ни было деньги и не переводить их на банковские счета по указанию незнакомых.

ОИОС по материалам управления по противодействию киберпреступности КМ УВД

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!

ОИиОС УВД по материалам УПК КМ УВД Могилевского облисполкома

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 либо оплачивает полностью приобретаемый товар и, как итог, 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.р., посредством 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.

По материалам УПК УВД Могилевского облисполкома

**Как не попасть на мошенников,
покупая запчасти к авто через интернет**

Основным видом регистрируемых киберпреступлений по-прежнему 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 автотранспортной техники и запасных частей.

Как правило, стоимость указанных товаров у таких продавцов гораздо ниже рыночной. Покупатель вносит предоплату либо оплачивает полностью приобретаемый товар, но остается без денег и без покупки.

Граждане, к сожалению, продолжают попадаться на уловки мошенников, а после обращаются за помощью к правоохранителям Могилевщины.

Вот несколько последних случаев.

Житель Добруша, 1992 г.р., обратился в милицию с заявлением о том, что 15 *апреля неизвестный с использованием глобальной сети «Интернет» на сайте «AV.by» обманным путем под предлогом продажи автомобиля завладел его 987 рублями.*

Могилевчанин, 1986 г.р., также попался на уловку мошенника. Через торговую площадку он нашел объявление о продаже автозапчастей и связался с указанным продавцом, после в мессенджере «WhatsApp» посредством фишинговой ссылки с его карт-счета было похищено 158 рублей.

640 рублей лишился житель Кличева, 1989 г.р., решивший купить автомобильные шины через интернет. 13 мая неизвестное лицо в социальной сети «Instagram» с учетной записи обманным путем под предлогом продажи товара похитило его деньги, переведенные за товар на лицевой счет банка.

17 мая неработающий житель Ивацевичского района Брестской области, 1997 г.р., сообщил в милицию о том, что 17 мая неизвестный через интернет на торговой площадке обманным путем, под предлогом продажи автомобилям «Iveco» завладел 970 рублями, переведенными на банковскую карту.

По всем указанным фактам следователями возбуждены уголовные дела.

Чтобы не стать жертвой мошенников, покупая автотранспортную технику и запасные части, важно быть бдительным и не поддаваться на сомнительные предложения. 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. Также не стоит вносить предоплату за покупку или услугу.

По материалам УПК УВД Могилевского облисполкома

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.

Управление по противодействию киберпреступности КМ УВД

Безопасное инвестирование: как уберечь от мошенников свои сбережения?

Все чаще в интернете встречаются предложения о быстром заработке путем вложения денежных средств в акции или криптовалюту. Казалось бы, все просто! Однако зачастую под видом специалистов в сферах криптовалюты, валютно-фондовых бирж и сотрудников администраций онлайн-казино скрываются мошенники.

С использованием различных мессенджеров злоумышленники создают аккаунты, где обещают доверчивым гражданам приумножить их сбережения.

Вот несколько примеров, как могут разворачиваться события:

1. Мошенники просят перейти по предоставленной фишинговой ссылке, которая переадресует пользователя на сайт, внешне схожий с криптобиржей/волютно-фондовой биржей. Далее – просят ввести личные данные, реквизиты банковских счетов и зарегистрировать аккаунт, чем предоставляют всю необходимую злоумышленникам информацию.

2. Мошенники уговаривают граждан перевести сбережения на банковские счета и ожидать, пока деньги «не начнут работать».

При любом исходе результат один: злоумышленники присваивают себе деньги доверчивых граждан и перестают выходить с ними на связь.

С помощью подобных схем под предлогом дополнительного заработка на онлайн-биржах жертвами мошенников стали жители Бобруйска и Белыничей.

После перехода по фишинговым ссылкам они лишились всех своих сбережений – более 20 000 рублей.

Схожим образом была обманута жительница Бобруйского района. После переписки со злоумышленником в одном из мессенджеров женщина лишилась 800 рублей.

Сотрудники милиции призывают граждан быть бдительными и напоминают о мерах безопасного общения в интернете: