Публикации на тему «Основные схемы кибермошенничеств»

1. Советуем гражданам внимательно относиться к рекламным играм в сети Интернет

Жительница города Светлогорска при просмотре социальной сети «Instagram» обратила внимание на рекламу о розыгрыше 150 рублей, который проводил один из белорусских банков. Чтобы получить деньги женщина перешла по предложенной ссылке и в открывшемся окне ввела свои паспортные данные и смс-коды, которые поступили на её мобильный телефон. В результате с карт-счета горожанки списалось более 500.

Следователями возбуждено уголовное дело по факту хищения путем использования компьютерной техники.

Сотрудники милиции напоминают:

Если Вам предлагают в сети Интернет поучаствовать в каком-нибудь розыгрыше, сначала ознакомитесь на официальном сайте организации, которая его проводит, с условиями рекламной игры.

Не под каким предлогом не вводите реквизиты своего паспорта или банковской карты на страницах ресурса, которые отображаются при переходе по ссылке. Сайт может оказаться «фишинговым». Мошеннические веб-ресурсы созданы для того, чтобы обманом заставить вас ввести личные данные в электронную платежную форму!

2. 26-летний речичанин взял кредитов на 12 200 рублей, думая, что помогает милиции

В конце ноября с 26-летним жителем Речицы по Вайберу связался неизвестный и представился сотрудником правоохранительных органов. Также по Вайберу в доказательство своих слов он сбросил фото удостоверения, после оказавшееся недействительным.

Далее, по известной схеме он рассказал, что якобы из другого города зафиксирован интерес со стороны преступников к карт-счету молодого человека – на него пытаются оформить кредит. Чтобы не допустить этого и помочь милиции выйти на потенциальных мошенников, реальный мошенник попросил парня оказать помощь. А именно: взять в банке, где тот обслуживается, кредит самому. Как

объяснил преступник, это поможет вычислить мифических злоумышленников.

Молодой речичанин последовал инструкциям и оформил на себя кредит на 4200 рублей. Затем установил на телефон приложение RustDesk, которое позволяет удаленно управлять гаджетом и, соответственно, проводить операции в интернет-банкинге. И передал логин и пароль тому, кто представился сотрудником милиции. Естественно, деньги, поступившие на счет, сразу были списаны. На недоумение парня мошенники ответили, что «операция по поимке преступников» продолжается, и деньги ему потом вернут, они сейчас «на обработке».

Дальше – больше: взявшиеся за речичанина киберпреступники попросили взять еще один кредит, на этот раз в другом банке. Когда на счет жертвы поступило 8 000 рублей, они также были списаны. Начав понимать, что происходит что-то не то, молодой человек напрямую спросил, мол, может, вы и есть мошенники? На что получил оскорбления, и диалог прервался. Только тогда 26-летний житель Речицы отправился в РОВД.

3. Хотела купить трактор в интернете - осталась без денег и техники

В минувшем декабре 49-летняя женщина-фермер из Кормянского района нашла на специализированной площадке в интернете объявление о продаже почти нового трактора по очень привлекательной цене.

Она связалась с продавцом через мессенджер. Тот утверждал, что предложение реально, но якобы из-за большого спроса продаст технику тому, кто первым переведет предоплату. Это смутило женщину, но после того, как собеседник прислал ей фотографии паспорта, последние сомнения пропали: она отправила неизвестному почти 17 тысяч рублей. Сразу после этого продавец перестал выходить на связь.

Следователями возбуждено уголовное дело по факту мошенничества, совершённого в крупном размере.

Оперативники установили, что паспорт на фото настоящий. Но его владелец сам ранее стал жертвой мошенников, которые теперь используют его данные для обмана других.

Чтобы не попасть в подобную ситуацию, не переводите деньги и не передавайте личные данные незнакомцам из интернета.

ОИОС УВД

4. Какие последствия могут наступить, если у мошенников окажутся личные данные паспорта

Гомельчанин долго искал себе работу по душе, рассылал резюме в разные фирмы и ждал заветного звонка от потенциального работодателя. Ему на «Viber» поступил звонок, мужчина сказал, что ознакомился с его резюме и готов предложить работу с достойной зарплатой. Для того чтобы начать процедуру оформления на работу, ему необходимы паспортные данные для формирования личного дела.

Доверившись собеседнику, соискатель отправил фотоизображение паспорта, а через некоторое время передал код, поступивший на мобильный телефон в смс-сообщении. Мужчина не обратил внимания на то, что код поступил из банковского учреждения.

После получения всех личных данных, злоумышленник с использованием Межбанковской системы идентификации (МСИ) прошел процедуру личной идентификации и получил доступ к расчетному счету, с которого перевел все деньги себе на расчетный счет.

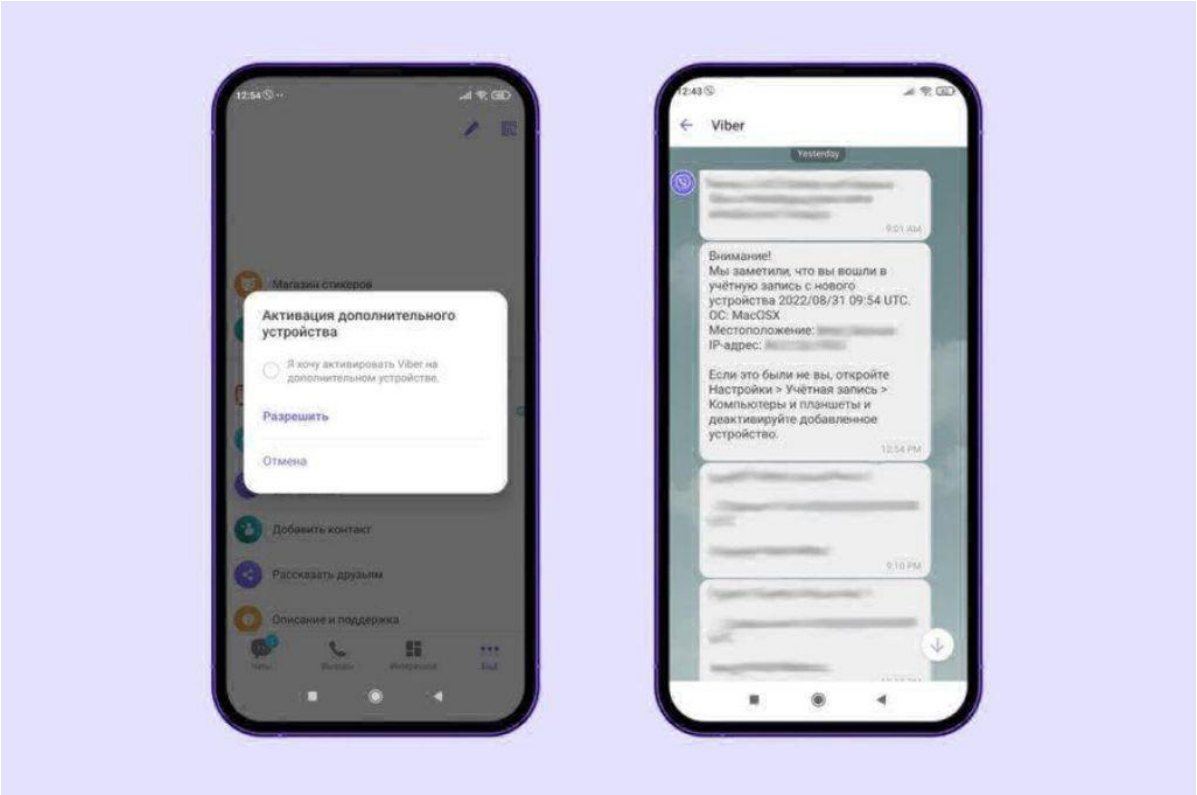
Такая схема интернет-мошенничества не редка в наше время. Какие еще последствия могут наступить, если у мошенников окажутся личные данные паспорта?

Самое опасное, что может ждать хозяина паспорта, данные которого утекли в сеть, – открытие кредита на его имя либо покупка товаров в рассрочку. Также с использованием паспортных данных можно зарегистрировать и купить доменные имена, которые затем используются для проведения сетевых атак, создать электронные кошельки или выпустить платежные карты для осуществления транзитных операций с украденными средствами или их обналичивания, создать аккаунты в онлайн-играх, биржах, букмекерских конторах в мошеннических целях.

Жертвами мошенников становятся как молодежь, которая зачастую легкомысленно относится к различным интернет-предложениям, так и наивные пенсионеры, не разбирающиеся в современных технологиях.

5. В Viber рассказали, как обезопасить свой аккаунт от мошенников

В Беларуси появилась новость о новой схеме мошенничества — злоумышленник активировал учетную запись пользователя Viber на другом устройстве, получив от пользователя подтверждение активации нового устройства. Таким образом, учетная запись пользователя не взламывается, пользователь сам на своем устройстве разрешает активацию ему не принадлежащего дополнительного устройства.



Новая схема мошенничества работает следующим образом:

Злоумышленник проходит процедуру активации учетной записи на новом устройстве: отправляет ссылку для подтверждения активации нового устройства пользователю-владельцу учетной записи. Пользователь, получая ссылку от неизвестного номера, открывает сообщение и кликает на на эту ссылку. После чего пользователь самостоятельно подтверждает активацию, нажимая “Я хочу активировать Viber на дополнительном устройстве” — тогда аккаунт пользователя активируется на устройстве мошенника. После этого пользователь получает от Viber сервисное сообщение с предупреждением о том, что его учетная запись была активирована на новом устройстве, включая информацию о типе устройства и его местоположении. Это делается, чтобы пользователь мог понять, что в его учетную запись был выполнен вход с другого устройства. И в случае, если это не он, — деактивировать новое устройство. В сервисном сообщении от Viber указано, как это сделать на основном мобильном устройстве (см. скриншот): «Если это были не вы,

откройте Настройки > Учетная запись > Компьютеры и планшеты и деактивируйте добавленное устройство». Этим способом пользователи могут в любое время деактивировать второе устройство.

Команда Viber напоминает, что ни в коем случае нельзя открывать ссылки, которые приходят вам от неизвестных пользователей, а также подтверждать активации новых устройств к вашей учетной записи, если это не вы пытаетесь активировать дополнительное устройство для своей учетной записи в Viber. Мошенники могут писать или звонить пользователям со специально созданных аккаунтов с использованием ненастоящего имени и аватара с целью выдать себя за официальных представителей той или иной организации — особенно часто это касается таких сфер как банковские услуги, телеком и пр.

Жертвами такого мошенничества, например, могут стать дети или пожилые люди, которые могут пройти всю процедуру активации: переходя по ссылкам, соглашаясь со всеми шагами активациинового устройства и не обращая внимания на сервисные предупреждения. Viber напоминает о необходимости быть внимательнее и осторожнее в digital-среде, а также помогать близким, если происходит что-то подозрительное.

Безопасность пользователей является одним из ключевых приоритетов для Viber. С 2016 года в Viber все основные функции защищены сквозным шифрованием по умолчанию, в том числе это касается личных и групповых чатов, личных аудио- и видеозвонков, обмена медиафайлами и безопасности всех связанных устройств пользователя. Мы продолжаем заботиться о безопасности наших пользователей и изучаем эту конкретную ситуацию с активацией учетной записи, чтобы предоставить пользователям еще больше информации и инструментов для защиты в таких случаях.

Комментарий предоставлен пресс-службой Rakuten Viber

6. В каких схемах могут участвовать подростки и какие последствия ждут «дропов» в дальнейшем?

7.

Все чаще в социальных сетях и мессенджерах пользователям стали приходить сообщения с предложениями без особых усилий за день заработать до 100 долларов. Что для этого нужно? Всего ни чего, оформить на себя банковскую карту в банке, на который укажет мнимый работодатель, и передать сообщением полученные реквизиты карты потенциальному работодателю.

Как правило, все общение проходит в сети Интернет без личного контакта. Истории, для чего нужна работодателю банковская карта чужого человека, различны. В основном это необходимость перевода денег на счета в Беларуси, а сам он не может, так как находится в другой стране.

Человек, согласившийся на такие условия сделки, становиться так называемым «ДРОПОМ» – подставным лицом в серых схемах кибермошенников. Дроп – этот тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу милиции.

Дропы бывают «разводные» и «неразводные». Отличие их только в том, что неразводные осознают всю тяжесть совершаемых им деяний и умышленно занимаются этим. В большинстве своем это студенты, школьники, малоимущие, которые нуждаются в финансах. Разводные «дропы» не знают о том, что идут на преступление. Они думают, что действительно работают, получают зарплату и т.д.

В каких схемах могут участвовать подростки?

Обналичивание денег в банкоматах: действия – принять деньги, снять деньги, взять себе процент, остальное переслать заказчику. Вот по такой нехитрой схеме и работают дропы.

Банковский перевод: предоставь мнимому работодателю свои реквизиты банковской карты, подождать когда на нее зачислят украденные деньги, переслать деньги на счет который укажет заказчик, оставить себе процент на банковской карте.

Пересылка товара: действия такие: дать свой адрес, принять посылку, переслать посылку на нужный адрес\отдать в руки (и такие есть), получить вознаграждение. Главное – наличие паспорта и прописки.

Дропы могут понадобится и для других дел. Например, покупка симкарт с помощью которых в дальнейшем совершаются преступления.

Какие последствия ждут «дропов» в дальнейшем?

Ответственность за такие действия наступает по ст. 222 УК Республики Беларусь. Незаконный оборот средств платежа и (или) инструментов

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений

незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, – наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, – наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

Ответственность наступает с 16 летнего возраста.

7. Будьте бдительны! Мошенники действуют под маской интернет-магазинов!

В августе месяце три жительницы Речицы решили воспользоваться в сети Интернет услугами интернет-магазина женской одежды. После того как товар был выбран, девушки начали переписываться с продавцом о способе оплаты. В переписке продавец настаивал на предоплате за товар, только после этого он сможет его выслать по указанным адресам. Не чувствуя подвоха, девушки перечислили на указанный злоумышленником расчетный счет более 200 рублей. В назначенный срок покупки речичанки не получили. В ходе дальнейшей переписки в сети Интернет продавец на обоснованные претензии со стороны девушек никак не реагировал. В настоящее время возбуждено уголовное дело по факту мошенничества, проводится проверка.

Советы как распознать фейковый интернет-магазин:

- Внимательно изучите сайт интернет-магазина. Если на нем отсутствует раздел «Контакты» - сразу проходите мимо. Иногда на фейковых страницах есть форма ввода вашего номера телефона и подпись вроде «Мы вам перезвоним». Если вы ввели свой номер телефона, не удивляетесь, что Вам потом могут перезвонить какие-нибудь сотрудники банка и сказать что у Вас одобренный кредит или Вы выиграли в лотерею 1 миллион долларов и чтобы его забрать необходимо перечислить сумму на определенный расчетный счет.
- Относитесь критично к отзывам, размещенным на сайте интернет-магазина, в основном они только хвалебные и не всегда правдивые.
- Скопируйте фото товара, размещенного на сайте, и вставьте в поиск по картинкам в браузере Google или Яндекс. Если поисковик выдает ссылки на этот же магазин и еще на два-три известных, это

нормально. Если же Вы увидите на экране неимоверное количество разноименных сайтов, причем картинка везде будет одна и та же, это почти наверняка мошенники.

- САМОЕ ГЛАВНОЕ! Никогда не соглашайтесь на предоплату за товар. Очень большой риск не получить его вовсе. Оплату производите только при получении товара (самовывоз, доставка курьером).

8. Под видом спецоперации мошенники выманили у мозырян более 120 тысяч рублей

Об этой схеме мошенничества уже сказано и рассказано довольно много. Вариаций немало, преступникам надо отдать должное, работают творчески, но в рамках выработанной схемы. Однако, в зависимости от ситуации, могут вносить и новые креативные идеи. Но финал таких историй всегда один – полная потеря денег.

В умело расставленную прохиндеями ловушку в июле попали мозыряне. Утром 20 числа жителю райцентра позвонили на мобильный телефон и представились персональным менеджером службы безопасности национального банка Республики Беларусь. Звонивший сказал, что прямо сейчас кто-то пытается похитить с карты мужчины деньги. Если тот хочет их сохранить, нужно немедленно переместить их в депозитную ячейку Нацбанка. Был продиктован номер счёта, на который обеспокоенный горожанин перевёл более 16-ти тысяч рублей.

Злоумышленники поняли, что клиент поверил и стали действовать по стандартной и отработанной схеме: идёт специальная операция милиции по поимки преступников, которые с банковских счетов у людей похищают деньги. Менеджер предупредил пожилого мужчину, что сейчас ему перезвонит руководитель данной операции МВД, который и проведет инструктаж по дальнейшим действиям.

Звонок действительно поступил. Целый полковник подтвердил о проведении оперативной комбинации, где задействованы сотни сотрудников. Он рассказал, что сам сейчас находится в Москве, вычисляет мошенников, а помощь в их поимке могут оказать только мозыряне. Якобы они сейчас являются ключевым звеном в этой операции. Для этого связь с ними будет держать менеджер, и потребовал все его требования и указания выполнять беспрекословно. А за деньги пусть не волнуются, после поимки всех бандитов им все вернут, и даже наградят. Для подтверждения полномочий

правоохранитель сбросил им в мессенджер фото своего служебного удостоверения. Как окажется впоследствии – подделка.

Долго указаний ждать не пришлось. Первым требованием было идти в один из банков и взять 7 тысяч рублей кредитных денег. Что жители райцентра и сделали. Злоумышленники также потребовали установить на свои телефоны и компьютер программу «AniDesk». Таким образом взяли под удалённый контроль управление карточками жителей Мозыря. После установки программы с карточки мозырянки сразу же списались почти 5000 рублей.

За последующие несколько дней муж и жена обошли несколько банков, где брали крупные суммы заёмных средств. Их сразу переводили на карточку одного из банков, с которых они мгновенно исчезали. Но их успокаивали – всё под контролем, все хранится в депозитной ячейке.

Денег требовали всё больше. Женщина положила на карточку свои личные сбережения – более 15 тысяч рублей. Они также исчезли в тот же день. Дошло до того, что на телефонах семейной пары стали заканчиваться деньги. Но мошенники их успокоили, сейчас поможем. И действительно, супруге на телефон перевели 20 рублей, мужу – 30-ть.

За пять дней спецоперации мозыряне перевели мошенникам почти 80 тысяч рублей. Но тем и этого оказалось мало. Под видом того, что их могут допустить к пользованию их деньгами, им нужно доложить туда ещё 10-ть тысяч, тогда у них будет доступ к деньгам. Наивные люди повелись и на это. Взяли имеющиеся накопления в долларах США, обменяли на белорусские рубли, и снова положили на карту, которой уже управляли.

После пошли штрафы за то, что муж отключил интернет, и они не могли дозвониться. За это потребовали 3000 рублей. Потом срочно понадобилась сумма для страховки ранее переведенных денег. На это понадобилось 5 тысяч.

Когда пришло время платить коммунальные услуги, денег не осталось. Но звонивший менеджер обрадовал, за отличную работу вам премия, и перевел им на карточку 340 рублей. Возникшую проблему удалось разрешить.

Но аппетит мошенников уже было не остановить. Люди сдали в ломбард все свои золотые изделия, оформили договор на продажу квартиры. Вырученные деньги и задаток в 3,5 тыс $ злоумышленники снова забрали с карт-счёта.

Только к 30 июля горожане заподозрили, что их, возможно, обманывают. К тому моменту они уже перевели мошенникам более

122000 рублей. После поступившего заявления в милицию следователями возбуждено уголовное дело по факту мошенничества.

9. Не попадись на удочку

Правоохранительные органы неустанно напоминают гражданам о мошенничестве с использованием современных технологий. Вот только число жертв нечистых на руку людей меньше не становится. Несмотря на все предупреждения, количество потерпевших на территории Наровлянского района увеличилось с нуля до четырех, при этом подозреваемые установлены только по двум фактам.

Так, неустановленное лицо в августе минувшего года, в ходе общения в соцсети «Одноклассники» под ником «Интернет магазин Милана», убедило жительницу Наровли перевести ему 74 рубля под предлогом продажи одежды. После чего завладело деньгами и товар не отправило. Эта же гражданка пострадала от недобросовестности еще одного продавца в тех же «Одноклассниках», теперь под ником «Модная ты». В этот раз она лишилась 60 кровно заработанных рублей. Еще один случай мошенничества с использованием соцсетей произошел в преддверии нового года. Под предлогом продажи мобильного телефона неустановленное лицо завладело 415 рублями другой жительницы райцентра.

А вот обратная сторона «медали». Уроженец Наровли, будучи ранее судимым, разместил объявление в социальной сети «ВКонтакте» в сообществе «Apple барахолка Мозырь» с предложением о продаже мобильного телефона. В ходе электронной переписки, убедил потенциального покупателя перевести на карту злоумышленника в качестве задатка 70 рублей. После чего перестал выходить на связь. И это одни из немногих случаев мошенничества, совершенных с помощью современных технологий.

Немало эпизодов, связанных с использованием фишинговых страниц и даже целых сайтов. Целью данной разновидности фишинга является получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код). Мошенники создают страницу, которая визуально очень похожа на страницу реально существующей компании или вовсе идентична ей. Размещают ее на сайте, название которого визуально тоже очень похоже на название реальной компании и имеет лишь незначительные различия.

Отправив такую ссылку пользователю, они ждут, когда он введет на ней свои данные. Как только это происходит, информация окажется в руках мошенников, и они смогут ее использовать по своему усмотрению. Для того чтобы узнать, что страница настоящая, необходимо в поисковике найти официальный сайт компании и сравнить написание с тем, которое вы видите на странице, которую вам кто-то выслал.

Алеся ЛИТВИН, Прыпяцкая праўда

10. Мошенник убедил пенсионерку установить программу удалённого доступа и похитил деньги с карточки

В Жлобинский РОВД поступило сообщение о том, что неизвестный, представившись сотрудником «Онлайн-гипермаркета», посредством телефонного звонка в приложении “Viber” убедил 63-летнюю пенсионерку установить программу удалённого доступа “AnyDesk” на мобильный телефон.

Впоследствии злоумышленник посредством программного обеспечения получил доступ к банковской платежной карточке на имя жлобинчанки. В итоге со счета женщины были похищены денежные средства в сумме более 700 рублей.

Возбуждено уголовное дело по статье 212 УК Республики Беларусь (Хищение путем использования компьютерной техники).

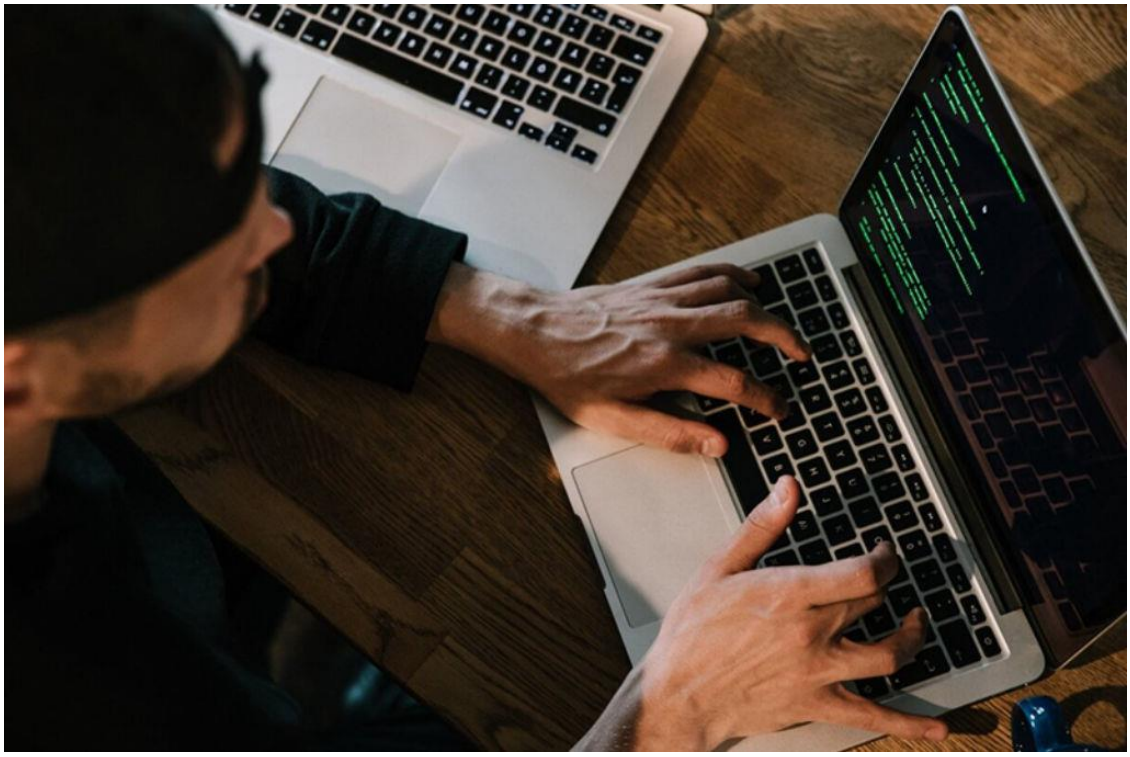
УВД Гомельского облисполкома напоминает о случаях телефонного мошенничества. Звонки, в основном, осуществляются с помощью мессенджеров. Злоумышленник в разговоре представляется работником банка, онлайн-магазина, контролирующих или правоохранительных органов и требует под любым предлогом предоставить информацию о банковской платежной карточке либо другие личные данные.

Чтобы не стать жертвой преступников, не сообщайте никому в телефонном режиме свои паспортные и иные личные данные, реквизиты счетов банковских платежных карт, а также содержание СМС-сообщений, поступающих с банковских учреждений.

По просьбе звонящего, не скачивайте никаких приложений на телефон. В случае поступления подобных звонков, окончите разговор и оставьте без ответа аналогичные входящие вызовы.

11. Жертвой кибермошенников может стать любой из нас, потому что никто не застрахован от обмана и манипуляций

За последние десятилетия число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Об этом свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц.



Жертвой кибермошенников может стать любой из нас, потому что никто не застрахован от обмана и манипуляций. Между тем существует достаточно способов обезопасить себя в интернете и противостоять телефонным мошенникам. Но сначала разберемся в основных видах киберобмана.

Не спешите читать

Не теряет своей актуальности так называемый «фишинг» – завладение реквизитами банковских карт с помощью фишинговых интернет-страниц, имитирующих популярные площадки объявлений. Через различные мессенджеры с гражданами, разместившими на площадке объявление о продаже различных товаров, велась переписка. В ходе общения потерпевшим предлагалось перейти по ссылке на фишинговую (поддельную) страницу, внешне схожую со страницей торговой площадки, и ввести реквизиты своей банковской карты для якобы отправки на их счет предоплаты. После ввода данных продавец денег не получал, а с его банковской карты списывались имеющиеся на ней денежные средства.

Чаще всего подделывают сайт торговой интернет-площадки «Kufar.by» и почтового сервиса «Белпочта», а также и остальных сайтов, на которых необходимо вводить либо логин и пароль от учетной записи, либо реквизиты банковской платежной карты. Один из последних случаев: 30 мая районным отделом Следственного комитета возбуждено уголовное дело по ч. 1 ст. 212 УК РБ в отношении неизвестного, который под предлогом покупки кондитерских изделий на интернет-площадке «Kufar.by» завладел реквизитами банковской платежной карты, принадлежащей мозырянину, 1981 г. р. С карты было похищено ни много ни мало 507,5 руб.

Еще один пример: в ходе переписки в мессенджере «WhatsApp» под предлогом покупки товара на площадке «Kufar.by» злоумышленник завладел реквизитами банковской платежной карты, принадлежащей работающему мозырянину, 1978 г. р., и похитил с нее 3702,72 руб.

А вот учащийся одного из учреждений образования Мозыря пошел еще дальше: он «развел» на деньги жительницу Москвы. Несовершеннолетний мозырянин использовал номер российского мобильного оператора в переписке в мессенджере «WhatsApp». Под предлогом покупки товара на сервисе «Youla.ru» он завладел реквизитами банковской платежной карты, принадлежащей россиянке, 1983 г. р. В итоге с карты было похищено 15000 российских рублей. Управлением Следственного комитета по Гомельской области в отношении несовершеннолетнего было возбуждено уголовное дело по ч. 2 ст. 212 УК РБ.

Инстаграм – популярная социальная сеть по продвижению аккаунтов граждан, позиционирующих себя или ремесленниками, или представителями физических магазинов. Эти аккаунты предлагают потенциальному потребителю уникальный товар. Вопрос только в том, кто скрывается за красивой картинкой: реальный продавец или мошенник? По оперативной сводке ОВД Мозырского райисполкома, за истекший период текущего года возбуждено 11 уголовных дел по факту мошенничества в инстаграме, и 6 дел проходят проверку.

Приобретая что-то через инстаграм, будьте предельно осторожны, потому что враз можно лишиться приличной суммы денег. Так, злоумышленник, используя учетную запись «Posydka_house», под предлогом продажи посуды завладел деньгами, принадлежащими мозырянке, 1980 г. р. Ничего не подозревающая женщина перечислила мошенникам 200 рублей на банковский счет ЗАО «Альфа-Банк». А через две недели, видимо, тот же мошенник

создал аккаунт «Posyda_house» и таким же образом обманул мозырянина, желающего приобрести посуду, на 250 руб.

Еще один продавец с аккаунта «Swimming_pool.by», только уже бассейна, «разбогател» на 490 руб., сыграв на доверчивости двух мозырян: в первом случае стоимость бассейна была 370 руб., и деньги переводились двумя транзакциями, во втором – 120 руб. Здесь немножко, там чуть-чуть – так и зарабатывать можно. Другой вопрос – что: деньги или срок?

Звонки с подвохом

Вишинг – это одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка.

Злоумышленники-«вишеры» обычно действуют так: на телефон жертве поступает звонок от «сотрудника банка», и оператор предупреждает: если прямо сейчас не будет предоставлена полная информация банковской карты ему по телефону, то карту заблокируют. Доверчивый пользователь, слыша подобную «угрозу», сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Один из недавних случаев: 30 мая на мобильный телефон пенсионера, жителя г. Калинковичи, поступил звонок через мессенджер «Viber». В ходе телефонного разговора с банковской платежной карты калинковичанина было похищено 217 руб.

Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться, всегда стоит лишний раз перепроверить информацию, обратившись к официальным ресурсам.

В любой непонятной ситуации главное – не паниковать. Помните: всегда всё можно проверить. Вежливо попрощайтесь с собеседником и позвоните на «горячую» линию организации, представителем которой назвался звонивший. Так вы легко сможете понять, был ли звонок обоснованным или вы чуть было не стали жертвой вишинга.

Ольга ЛАСУТА, www.mazyr.by

12. Регистрируются случаи интернет-мошенничеств, связанные с продажей билетов в театр и кино

С апреля месяца в Гомельской области все чаще стали регистрироваться случаи совершения интернет-мошенничеств,

связанные с продажей билетов на театральные постановки и киносеансы.

В мае месяце молодой парень из Гомеля, как и многие современные парни, решил познакомиться с девушкой через сеть Интернет. Наткнулся на профиль приглянувшейся ему представительницы прекрасного пола. Общение перешло в мессенджер «Telegram». Через некоторое время девушка сама предложила посетить кинотеатр, при этом настойчиво предлагая купить билеты на понравившийся ей фильм через определенный сайт, ссылку на который направила сама. Ничего не подозревающий молодой человек перешел по ссылке и ввел реквизиты своей банковской карты, думая, что оплачивает билеты в кино. После оплаты жертва, естественно, не получила никаких билетов, и осталась с нулевым балансом на счету. В итоге парень не досчитался более 300 белорусских рублей. Возбуждено уголовное дело по ст. 212 УК Республики Беларусь, ведется расследование.

Только за 2 месяца зарегистрировано 8 подобных случаев интернет-мошенничеств.

Фейковые сайты театров и кинотеатров выглядят почти так же, как настоящее: на них размещается описание спектаклей (фильмов) нового сезона, афиша, а также уведомление о возможности покупки билетов онлайн. В основном билеты в театр (кино) предлагали приобрести новые знакомые после общения в сети Интернет.

Приобретайте билеты только на проверенных сайтах театров и кинотеатров, не переходите по ссылкам, предоставленным Вам в сети Интернет.

Самый надежный способ защититься от такого рода мошенничества – это осуществлять покупку билетов в кассах театров и кинотеатров.

13. Расскажите своим пожилым родственникам о схеме мошенничества со звонками

Дети и внуки, огромная просьба именно к вам. Расскажите своим пожилым родственникам об этой схеме мошенничества. Кто, как не мы можем и просто обязаны защитить их от мошенников.

Схема обмана простая. Вам звонит неизвестный и представляется дочерью, сыном или внуком. Далее он говорит о том, что виноват в ДТП, ему грозит уголовная статья и лишения свободы. Вопрос можно решить, заплатив потерпевшим. Затем трубку берет «представитель силового ведомства». Он подтверждает факт

происшествия, а далее преступники обрабатывают жертву так, что та отдает огромные суммы денег.

Совсем недавно в такую ловушку попала 65-летняя гомельчанка. Она передала мошенникам 5000 рублей за непривлечение к ответственности невестки, якобы совершившей ДТП. И подобных фактов уже десятки.

Предупреждаем! В случае поступившего подобного звонка, немедленно прекратите беседу. Перезвоните родственнику, который якобы попал в ДТП. И ни в коем случае не отдавайте никому свои деньги!

ОИОС УВД

14. Фишинг. Жительница Гомеля недосчиталась на балансе своего лицевого счета 430 рублей

Торговые интернет-площадки продолжают привлекать мошенников.

В милицию обратилась жительница города Гомеля и сообщила, что после размещения своего объявления о продаже куртки ей на мобильный телефон в мессенджере Вайбер пришло сообщение от потенциального покупателя, который готов был сразу оплатить товар, чтобы он не достался кому-нибудь еще. При этом покупатель настаивал на оплате товара удобным ему способом. Для этого он сбросил ссылку потерпевшей, для заполнения данных по сделке. Не чувствуя подвоха, гомельчанка перешла по полученной ссылке и ввела данные своей банковской платежной карты в открывшемся окне. Дальше дело техники. Спустя некоторое время жительница Гомеля недосчиталась на балансе своего лицевого счета 430 рублей.

Милиция рекомендует!

К любым операциям, производимым с использованием Вашей банковской карты, относится максимально внимательно и осторожно. Терять бдительность никогда нельзя.

Для оплаты покупок в Интернете завести отдельную карту и не хранить на ней много денег.

Если Вам прислали ссылку на почтовый ящик, в мессенджер или SMS-сообщением, то, независимо от того кто прислал, прежде чем ее открывать, следует особенно внимательно проверить доменное имя. Сделать это можно отыскав в интернете официальный сайт под названием 2ip.ru. При проверке обратите внимание на информацию о дате регистрации домена, у фишинговых сайтов это обычно от нескольких дней до нескольких месяцев.

УПК УВД

15. Банк не осуществляет рассылку своих мобильных приложений в Viber или Telegram

Беларусбанк предупреждает о возможном новом способе мошенничества, с которым могут столкнуться пользователи приложения М-банкинг.

Работает схема следующим образом. Злоумышленники от имени банка направляют в месенджерах Viber или Telegram фишинговое сообщение с информацией о якобы возможной блокировке мобильного приложения банка официальными магазинами приложений.

Далее в сообщении может содержаться предложение установить (в целях сохранения работоспособности мобильного приложения) на ваш смартфон новую версию приложения из прикрепленного файла, который является вредоносным.

Обращаем внимание! Банк не осуществляет рассылку своих мобильных приложений в Viber или Telegram. Просим вас осуществлять установку М-банкинга только из официальных источников — магазинов приложений Play Market и App Store.

УПК УВД

16. В VK появился новый способ взлома страницы

В последнее время злоумышленники стали использовать новый способ получения полного доступа к странице VK путем использования социальной инженерии.

Схема выглядит следующим образом:

Пользователю приходит личное сообщение, от якобы "системы" со следующим содержанием.

Мы обработали вашу заявку на создания архива переписок Вашей страницы.

Архив будет выслан на вашу почту [ВАШ EMAIL] в течении суток. Если заявку подали не Вы, немедленно отмените запрос: [РЕДИРЕКТ VK НА ФИШИНГ РЕСУРС]. Сервис работает в тестовом режиме, мы будем продолжать улучшая работу.

Естественно пользователь переходит на фишинговый ресурс через скрытый редирект VK vk.com/away.php?to= что-бы отменить "запрос", где ему предлагают войти в свой аккаунт VK, таким образом злоумышленник получает полный доступ над вашей страницей. Будьте внимательны.

УПК УВД

17. Осторожно: мошенники стали использовать приложение «AnyDesk»

Цифровые технологии стремительно и необратимо меняют мир. Люди охотнее общаются в соцсетях, чем при личных встречах, с помощью Интернета совершают покупки, оформляют услуги… И порой становятся жертвами аферистов – несут финансовые потери. Находчивость мошенников поистине не знает границ. В их арсенале появился ещё один способ обмана – с использованием приложения «AnyDesk».

Для начала коротко – о программе. Наверняка о ней многие знают, но далеко не все. «AnyDesk» позволяет получить удалённый доступ с одного устройства к другому. Применяется, как правило, в профессиональной среде, для помощи знакомым, взаимодействия с домашним или служебным компьютером. Пользователь собственноручно загружает программу на своём устройстве и разрешает получить доступ к своей системе кому-то ещё. Так появляется возможность совершать любые действия на этом компьютере у другого человека. Например, отправлять сообщения, передавать файлы, удалять приложения и т.д. Всё создано по принципу: скачал, запустил и пользуйся. Легко и удобно. Для интернет-мошенников, к сожалению, тоже. Подобная программа стала активно ими использоваться для получения доступа к компьютерам или мобильникам своих жертв.

Один из разводов – звонок от лжесотрудника банка с предложением установить на телефоне приложение «AnyDesk». Как аргумент – «для защиты», «в целях безопасности», «чтобы получить доступ к новым услугам», «установить антивирус» и т.д. Понятно, что чаще на такие легенды ведутся те, кто не знает, для чего в реальности предназначена данная программа. Злоумышленники пользуются доверчивостью и невнимательностью людей, их слабым пониманием информационной безопасности. Согласился человек – и тем самым предоставил доступ к своему устройству, в том числе к мобильному банкингу, что позволяет жуликам похищать деньги.

Именно на такую уловку буквально на днях попалась жительница Брагина, у которой раздался звонок по вайберу.

– Неизвестный, используя абонентский номер белорусского оператора сотовой связи и выдавая себя за сотрудника Белагропромбанка, убедил женщину скачать на мобильный телефон

приложение «AnyDesk Remote Control». И таким образом завладел сведениями, предназначенными для входа в мобильный банкинг, персональными данными банковской платёжной карты. С карт-счёта потерпевшей было похищено 770 рублей.

Чтобы не попасться на обман и не стать жертвой аферистов, сотрудники правоохранительных органов призывают граждан быть бдительными. И в очередной раз доводят до сведения жителей района, что наиболее распространёнными способами интернет-мошенничеств являются:

Объявления о продаже. Лжепродавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

Объявления о покупке. Лжепокупатели спрашивают реквизиты банковской карты и (или) смс-код (якобы для перечисления денег за товар) либо просят перейти по направленной ими ссылке, где необходимо указать реквизиты своей карты. После получения этих данных преступники похищают деньги со счёта жертвы.

Звонок из банка, милиции и т.д. Злоумышленники звонят на телефон и представляются сотрудниками банка, правоохранительных органов или других государственных служб, сообщают о попытках совершения подозрительных операций и предлагают помощь в их отмене. Убеждают предоставить реквизиты банковской платёжной карты или просят установить приложения «AnyDesk», «TeamViewer», позволяющие получить доступ к мобильному телефону и банковскому счёту жертвы. Лжесотрудники службы безопасности могут также предлагать поучаствовать в поимке преступников, для чего просят гражданина оформить кредит и положить определённую сумму на якобы секретный счёт. После перевода денег ими распоряжается преступник.

Самый лучший способ защитить себя от таких мошенников – не сообщать данные банковской карты по телефону неизвестным лицам, даже если они представились сотрудниками банка, милиции и т. д. Не следуйте инструкциям незнакомых людей, полученным по телефону. Не переходите по ссылкам, полученным от кого-либо в сети Интернет. А при продаже или покупке товара общение ведите только на официальном сайте торговой интернет-площадки, товар желательно передавать или получать при личной встрече.

Валентина БЕЛЬЧЕНКО