## «Способы обмана в сети Интернет.»

1. **Виды мошенничества.**
2. **Основные схемы интернет- мошенничеств.**
3. **Дроппы.**
4. **Как уберечь себя и своих близких от киберпреступников.**

**1.Виды мошенничества.**

К числу самых популярных видов «обмана» в сети Интернет можно отнести «Фишинг», «Вишинг» и «Смишинг»- это мошеннические схемы, в которых для кражи личных данных с целью дальнейшего взлома банковского аккаунта и незаконного списания средств используются интернет- технологии. Основная цель у всех схем одна- получить у своей потенциальной жертвы конфиденциальную информацию.

**Фишинг-** (*перевод с англ. – рыбная ловля*) Некий вид получения злоумышленником секретной информации. Такими данными могут быть номер и код банковской карты, логин и пароль, от какого либо сервиса. В основном такой вид используют, чтобы получить доступ к онлайн - банкингу или электронному кошельку жертвы в той или иной платежной системе и вывести счета на посторонние счета. В качестве своеобразной «удочки» преступники используют специально созданный интернет сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве «наживки»- некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.

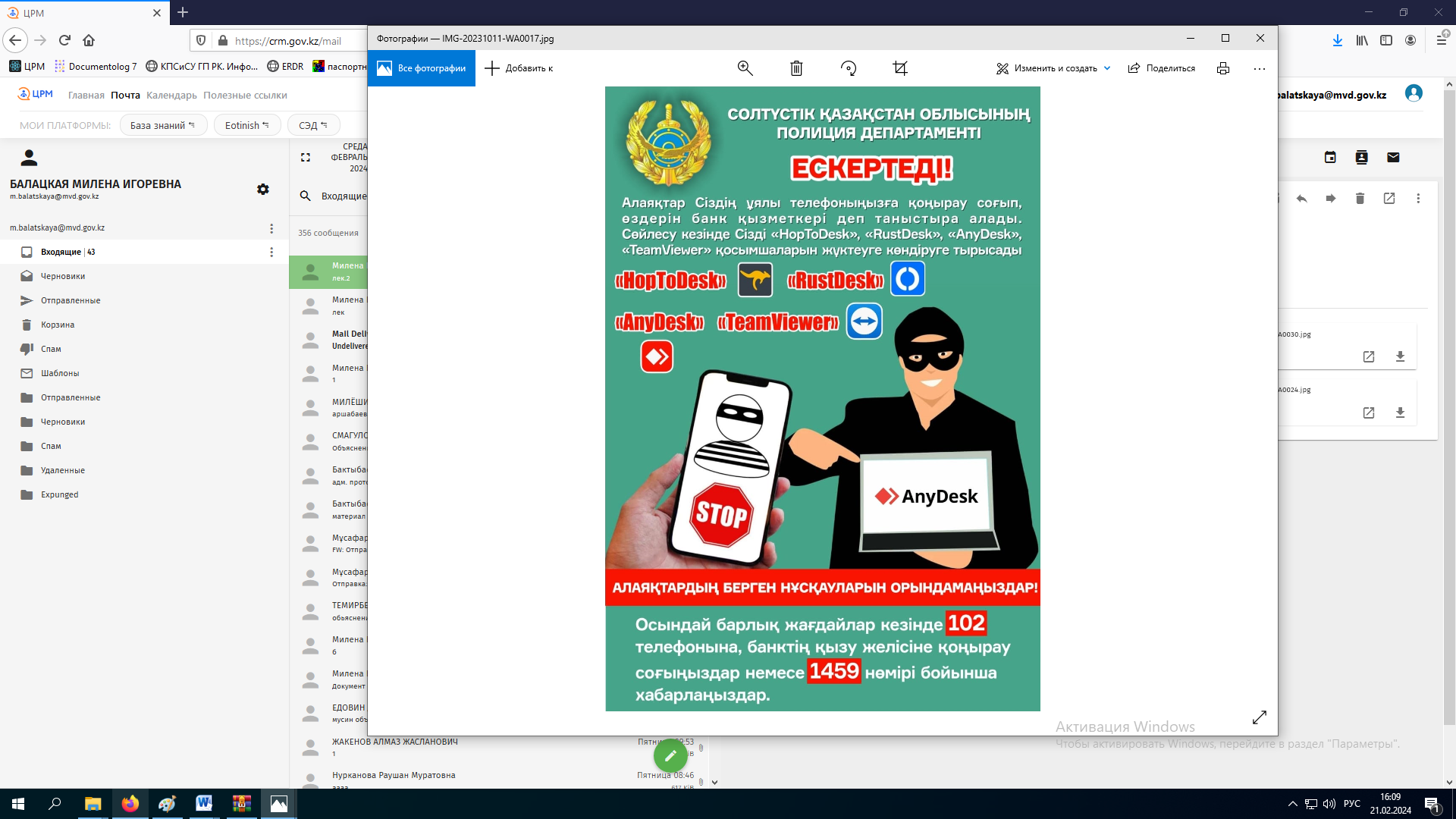
**Вишинг-** устная разновидность мошенничества, при которой злоумышленники, используя телефонную коммуникацию под разными предлогами стимулируют людей к совершению действий якобы в собственных интересах. Киберпреступники намеренно создают условия с целью побудить ничего не подозревающих жертв добровольно предоставить ценные личные данные, такие как анкетные данные, номера телефонов, реквизиты банковских карт и т.д. Во многих случаях звонящие являются самозваными экспертами или специалистами в различных областях. Киберпреступники могут представляться компьютерными специалистами, банковскими сотрудниками, сотрудниками правоохранительных органов.

**Смишинг-** данная преступная схема направлена на переход пользователем по вредоносной ссылке из СМС – сообщения, которое может иметь вид от лица известного банка, знакомой компании или быть просто об оповещении о внезапном выигрыше в лотерею или в крупную акцию. Примерно данное сообщение будет выглядеть так: «Подписка на платный сервис «Курс валют онлайн» прошла успешно. С вас будет изыматься ежемесячная комиссия. Для отказа сервиса пройдите по ссылке». Далее после перехода по ссылке пользователь переходит на фишинговый сайт, где ему предлагается ввести данные банковской карты.

**2.Основные схемы интернет- мошенничеств.**

**1. Телефонный звонок, где киберпреступники представляясь сотрудниками банковских учреждений,** сообщают, что неизвестные лица пытаются оформить кредит. Далее сообщают, что якобы для предотвращения оформления кредита, необходимо сообщить им номер банковской карты, CVV-код и скачать приложения удаленного доступа «Ру Деск», «Эни Деск» или «ХопТуДеск». После скачивания жертва диктует мошеннику коды доступа к данному приложению. Далее мошенник удаленно самостоятельно управляет всеми мобильными приложениями установленными в сотовом телефоне жертвы. Самостоятельно оформляет кредит и переводит денежные средства. В других случаях жертва самостоятельно оформляет кредит. Как правило похищенные денежные средства перечисляются на третьих лиц, которые находятся в другой области.

*Таким примером является случай произошедший с 63-летней жительницей областного центра в начале октября т.г., в вечернее время к ней на сотовый телефон позвонил неизвестный мужчина, который представился сотрудником Национального банка, пояснил, что мошенники оформили на ее имя кредит в сумме 3 000 000 тенге и порекомендовал скачать приложение «Хоптудеск», якобы для того, чтобы мошенники не смогли получить денежные средства с оформленного кредита. Далее следуя инструкциям, потерпевшая скачала к себе на мобильный телефон указанную программу. Через некоторое время с ее счета исчезли находившиеся там денежные средства в сумме 740 000 тенге. После чего она направилась в отделение банка и поняла, что стала жертвой мошенников.*

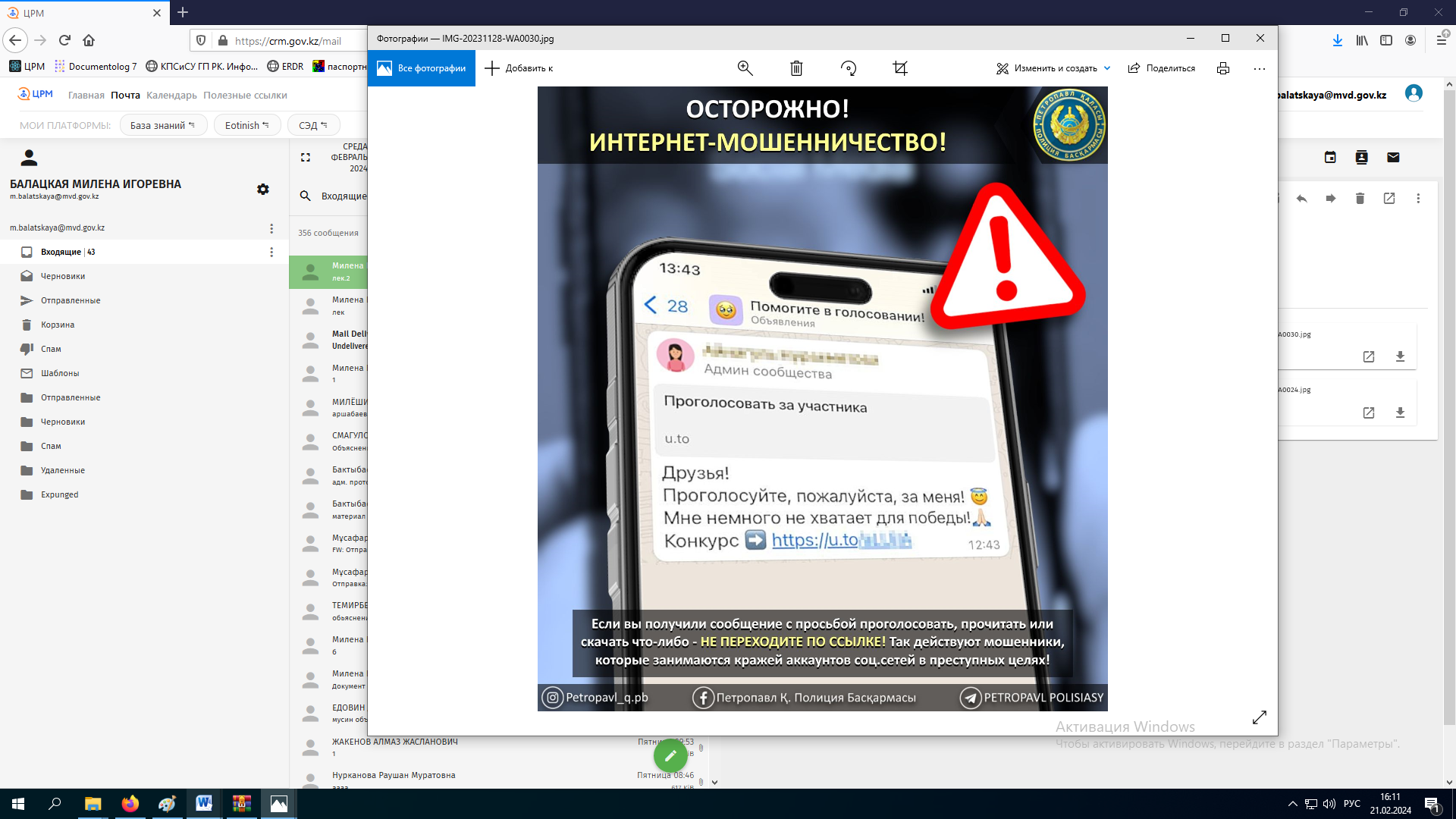
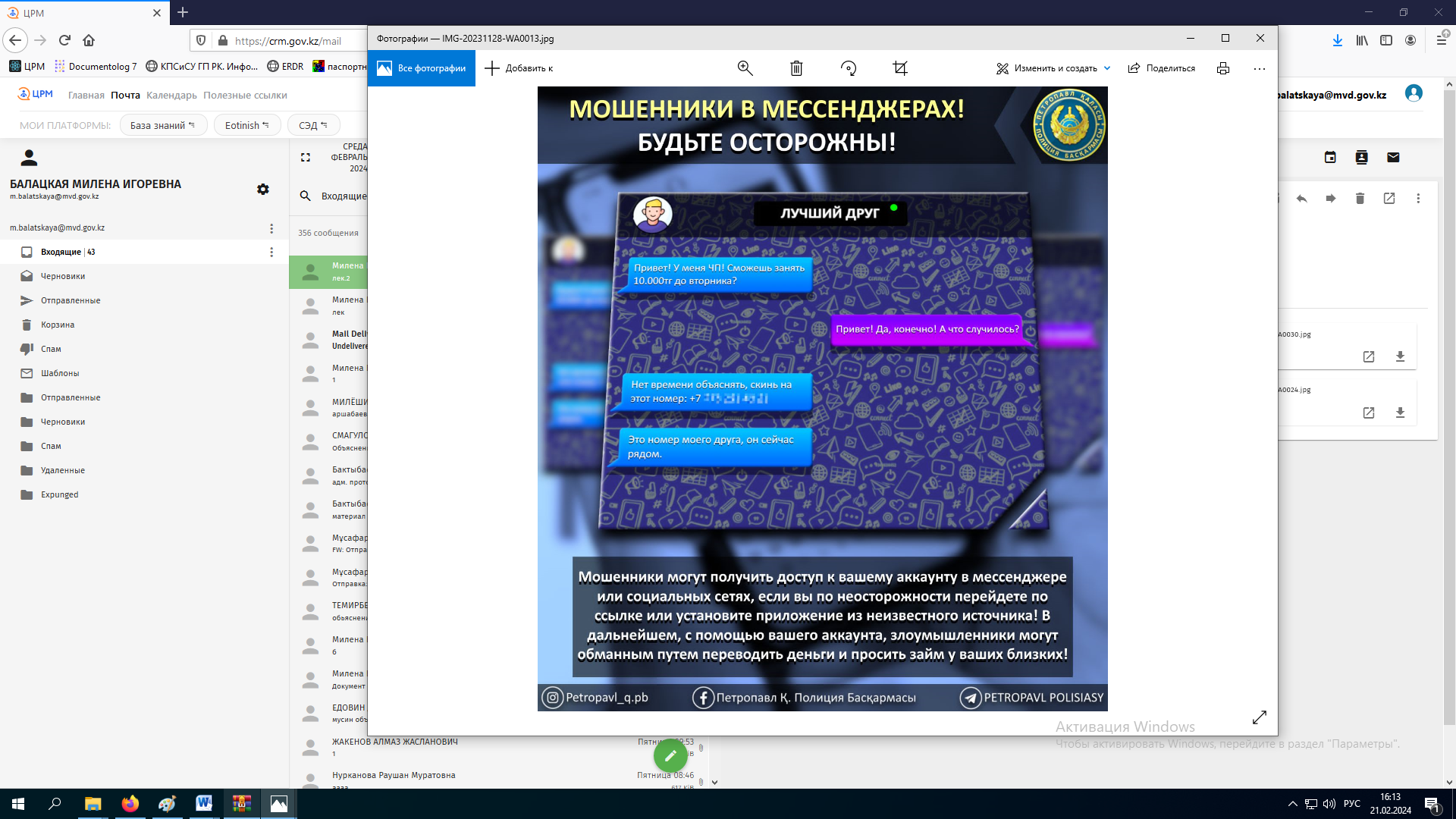
**2. Размещение фейковых объявлений на популярных интернет площадках.** Как правило, мошенники используют сайты с большим количеством подписчиков и положительными отзывами, привлекают своих жертв невысокой ценой, быстрым предоставлением товара или услуги. Киберпреступники создают сайты двойники, меняя локацию. Покупателей просят внести частичную или полную предоплату на счета, которые обычно оформлены на третьих лиц. Также на сегодняшний день получает свое распространение вид мошенничества при котором лицу, осуществляющему продажу товара на сайте «Олх», на сотовый телефон звонит «покупатель» и предлагает оформить покупку через курьерскую службу доставки, в дальнейшем отправляют ссылку на сайт-двойник на котором необходимо оставить реквизиты банковской карты. На данном сайте отсутствует такая услуга.

**3. Звонки от сотрудников правоохранительных служб. К**иберприступники звонят своим потенциальным жертвам (как правило звонок на стационарный телефон людям пожилого возраста), представляются сотрудниками полиции и сообщают, что по вине ваших детей или внуков совершено ДТП и для не привлечения их к уголовной ответственности, необходима выплатить крупную сумму денежных средств. После чего мошенники, действуя в группе лиц, играя определенную роль сына, дочери, внука или внучки своей потенциальной жертвы, по телефонному разговору просят помощи, сообщают, что если не выплатить крупную сумму денежных средств, они будут привлечены к уголовной ответственности. Далее отправляют на адрес своей жертвы кур**ьера –дроппа** для передачи денежных средств.

**4 Звонки от лиц представителей сотовой связи.** Сообщают о том, что истекает срок использования абоненского номера, сообщают, что необходимости перейти по ссылке продиктовать код, который указан в СМС сообщении, в случае отказа, данный номер будет заблокирован. Данный код- код подтверждения оформления кредита. Запомните- у сим карты нет срока годности.

**5.** **Сообщение от сотовой связи с иформацией о выйгрыше денежных средств.** Зачастую жертвами данной схемы становиться обычные граждане, которым приходит смс сообщение от якобы представителей сотовой связи, с указанием того, что их абонентский номер учувствовавший в розыгрыше, выиграл денежный приз, для получения которого, необходимо перейти по указанной в сообщении ссылки. Далее перейдя по ссылке, необходимо заполнить, в предложенной форме, реквизиты банковской карты, после заполнения, мошенниками похищаются ваши денежные средства. Не переходите по сомнительным ссылкам, указанных в смс сообщениях от лиц или организаций с которыми у вас нет и не было договорных отношений.

**6.** **Сообщение о голосовании на конкурсе. Фейковое размещения о обязательной выплате денежных средств гражданам от государства с указанием ссылке. Сообщение –просьба проголосовать за участника конкурса.** Киберпреступники используют в подобных сообщениях и публикациях - переход по ссылкам, которые являются фишинговыми- вирусными, с целью доступа к вашем данным и списания денежных средств.

**3.Дроппы**

Дроп или дропперы - это люди которых используют мошенники для достижения своей цели. Они не являются инициаторами преступлений, а выполняют указания, получая за это денежные средства. Являются низшей ступенью в данной схеме. Дроппы участвуют во всех схемах, по незаконному обналичиванию чужих денежных средств. Иногда люди осознано соглашаются на такую работу, но в других случаях компания может так шифроваться, что не возможно узнать, что вы вовлечены в нелегальные схемы. Мошенники размещают объявления в социальных сетях с заманиваемым предложением: где предлагают заработать много денег за короткий срок и за минимум усилий, не выдвигают особых требований к кандидату и принимают без опыта. Необходимо быть внимательным: под такой вакансией может скрываться мошенническая махинация. Обычно данная работа связана с переводом или обналичиваем денежных средств. Поэтому ни в коем случае не нужно откликаться на такие вакансии, так как можно оказаться соучастником преступления. Чаще всего дроппами становятся студенты, безработные. В предложениях работать дроппером есть некоторые отличительные особенности

1.Рассматриваются соискатели, без какого либо образования и опыта,

2.Работа, связана с переводом либо обналичиванием денежных средств

3.полная удаленная занятость, нет необходимости являться в офис для оформления документов

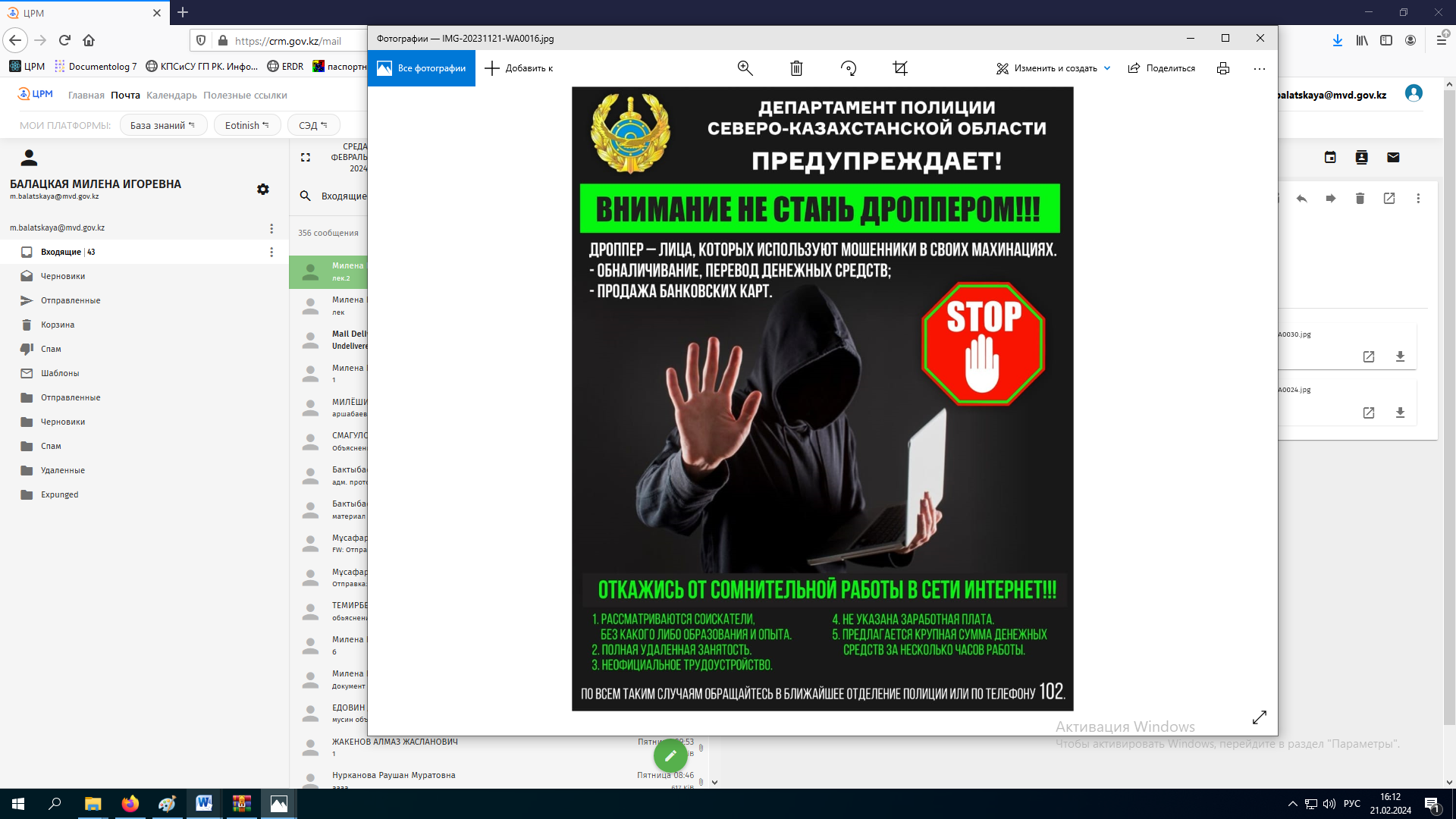
4. Неофициальное трудоустройство

5. Не указана заработная плата

6. Предлагается крупная сумма денежных средств за несколько часов работы.

7. Покупка банковских карт.

Как правило жертвы мошенников находят объявление о покупки банковских карт. Далее мошенники приобретают за определенную стоимость у своих жертв (студентов) банковские карты, через которые в последующем переводят денежные средства, добытые преступным путем. Следовательно, официальный владелец банковской карты (студент) становиться соучастником преступления. После совершения нескольких денежных переводов, киберпреступник возвращает банковскую карту владельцу. Владелец банковской карты несет определенную ответственность. В гражданском порядке, по решению суда и после заявленного иска потерпевшим лицом, владелец карты должен возместить причиненный ущерб.



**Как уберечь себя и своих близких от интернет-мошенников:**

- При покупке товаров в сети интернет рассматривайте приобретение товара только на проверенных сайтах. Убедитесь, что это не сайт двойник, а официальная страничка. Очень часто злоумышленники создают похожие сайты, изменяя только описание ресурса, используют логотипы известных банков, а также популярных брендов, это является одним из излюбленных способов обмануть человека. В данной ситуации, если у Вас просят предоплату за товар необходимо очень внимательно изучить условия предоплаты. Мошенник может отправить фото удостоверения личности, которое нашел в сети интернет, или получил обманным путем у другого лица. Также тревожным звонком при данной схеме является то, что покупатель настойчиво предлагает связаться только посредством социальных сетей. Свяжитесь видеозвонком и посмотрите действительно ли это тот человек, совпадают ли данные с документов и банковской карты. Посмотрите все комментарии и отзывы как о товаре, так и о поставщике. Если заказываете товар с другого города, в этом случае попросите родственников, знакомых проверить товар, имеется ли он в наличии и соответствует ли предъявляемым характеристикам;

- если Вам звонят с банка, представляются менеджером или сотрудником службы безопасности и сообщают, что по Вашей карте производится перевод денежных средств в другой город, страну и предлагают перевести денежные средства на застрахованный счет, необходимо прекратить разговор, незамедлительно перезвонить на горячую линию своего банка и сообщить о данной ситуации. Ни один сотрудник банка не будет звонить клиентам и интересоваться конфиденциальными данными, так как они им известны. Сведения о счетах, номер карты и контрольные цифры на обороте карты это данные, которые защищены банковской тайной. Если Вы сообщите данную информацию третьим лицам, а также смс с кодом пришедшим на телефон денежные средства незамедлительно будут сняты с банковской карты. Важно понимать, что в этой схеме мошенники используют элемент неожиданности, в ходе разговора используют банковские термины, разговор заранее продуман и спланирован.

**Напоминаем, что сотрудники банковских учреждений в телефонных разговорах не уточняют у своих клиентов номера и коды банковских карт, так как они им известны.**

**Чтобы проверить законность сообщения от имени банка, позвоните в банк по официальному номеру телефона.**

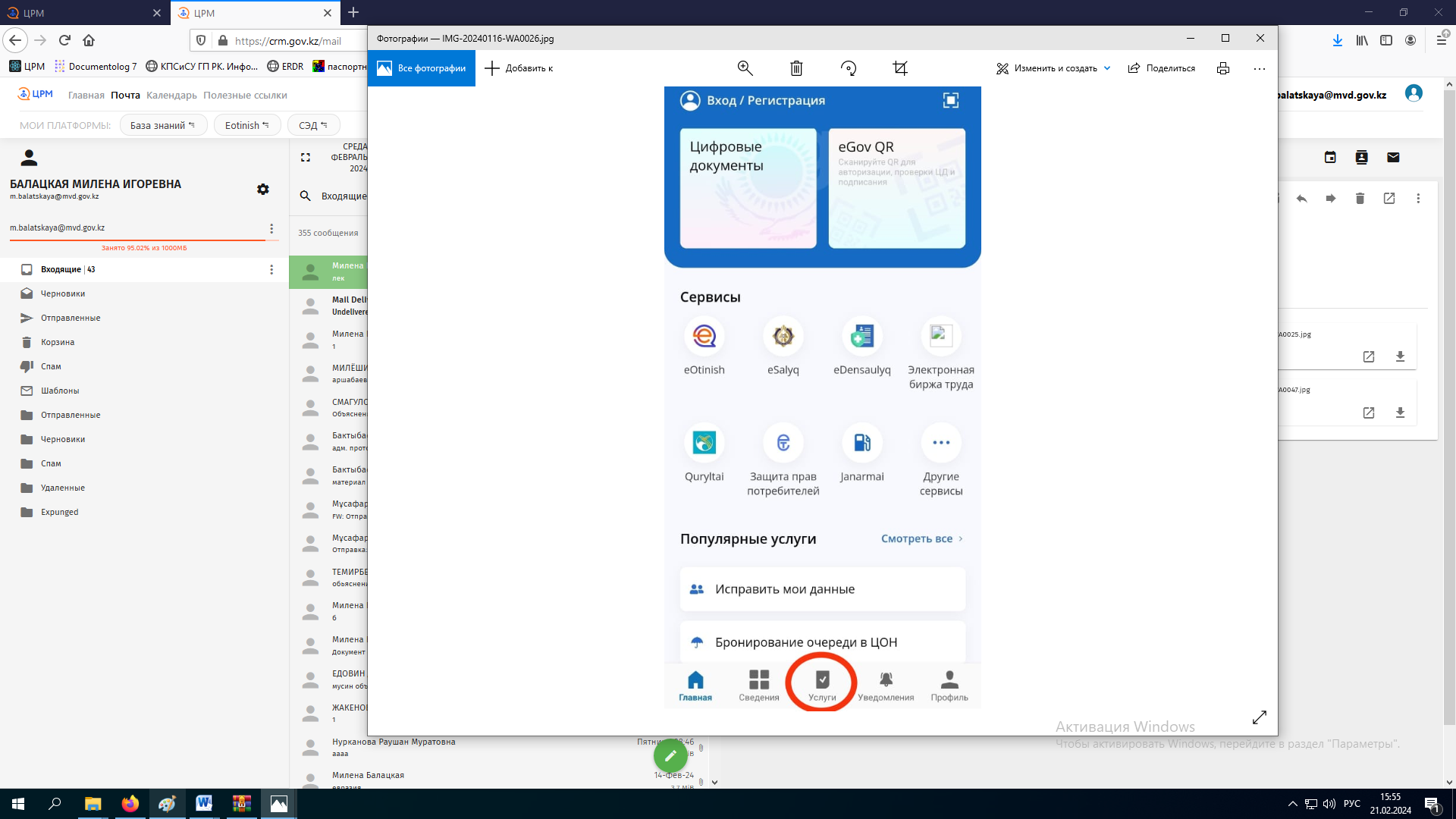
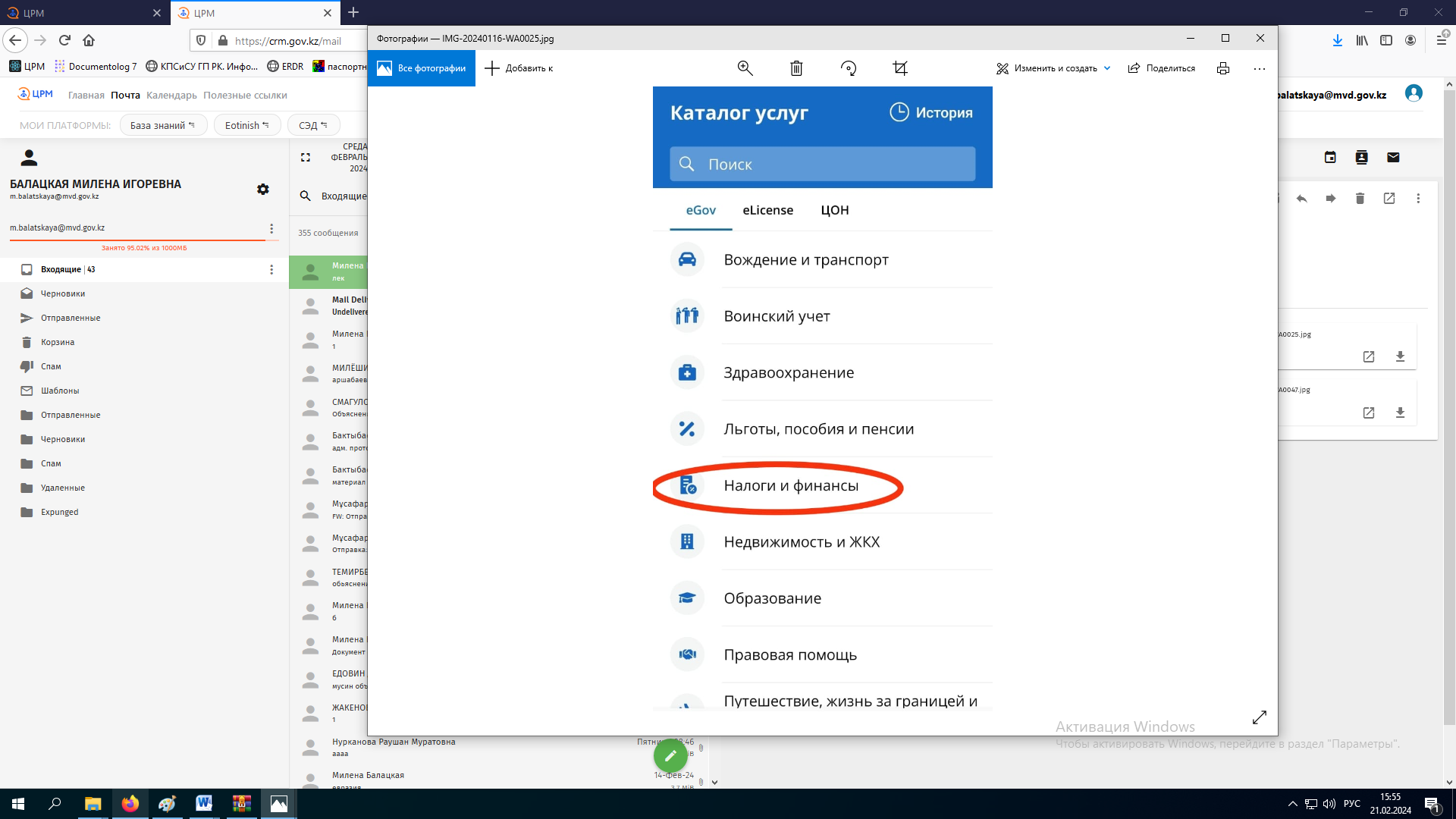
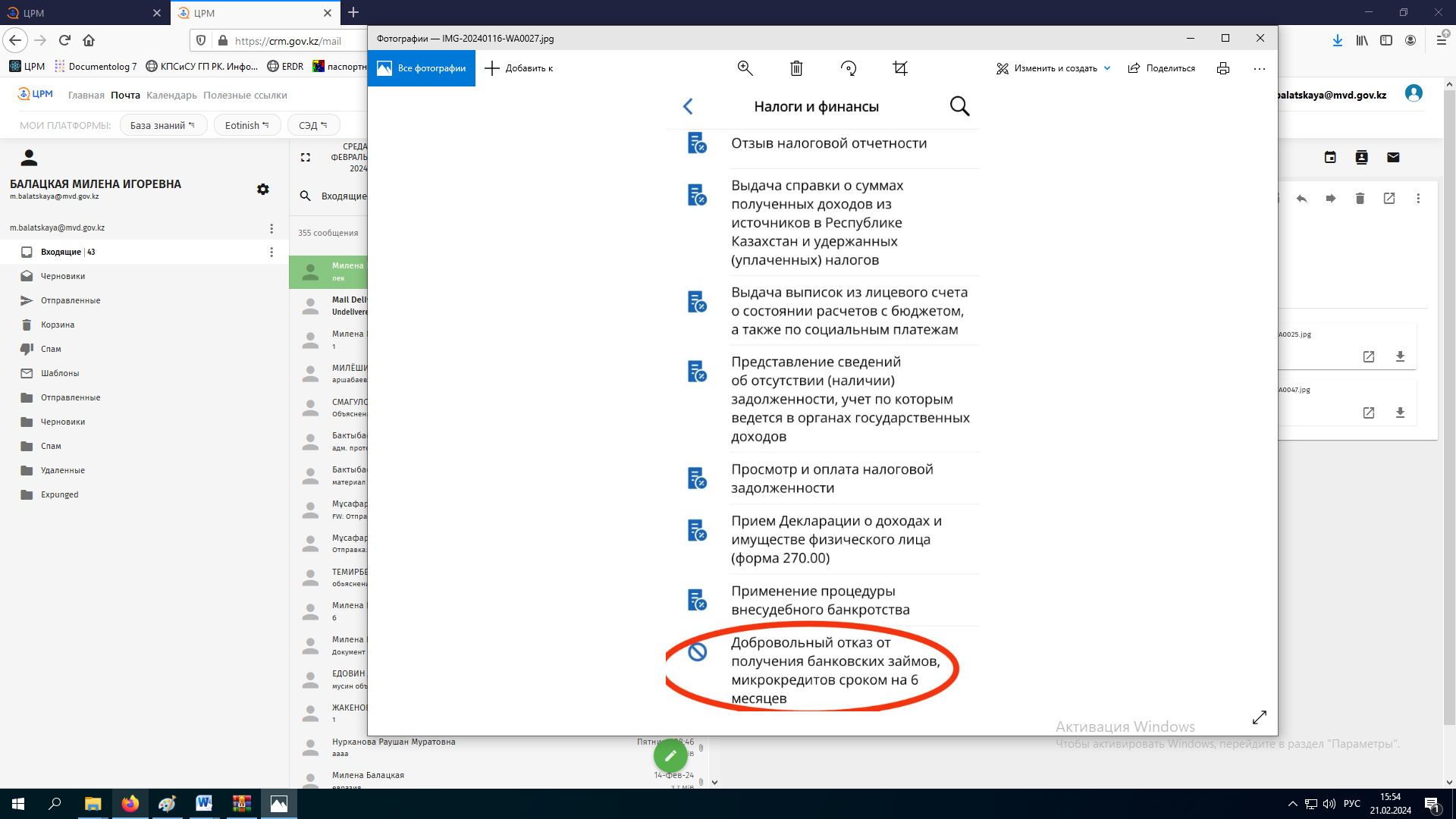
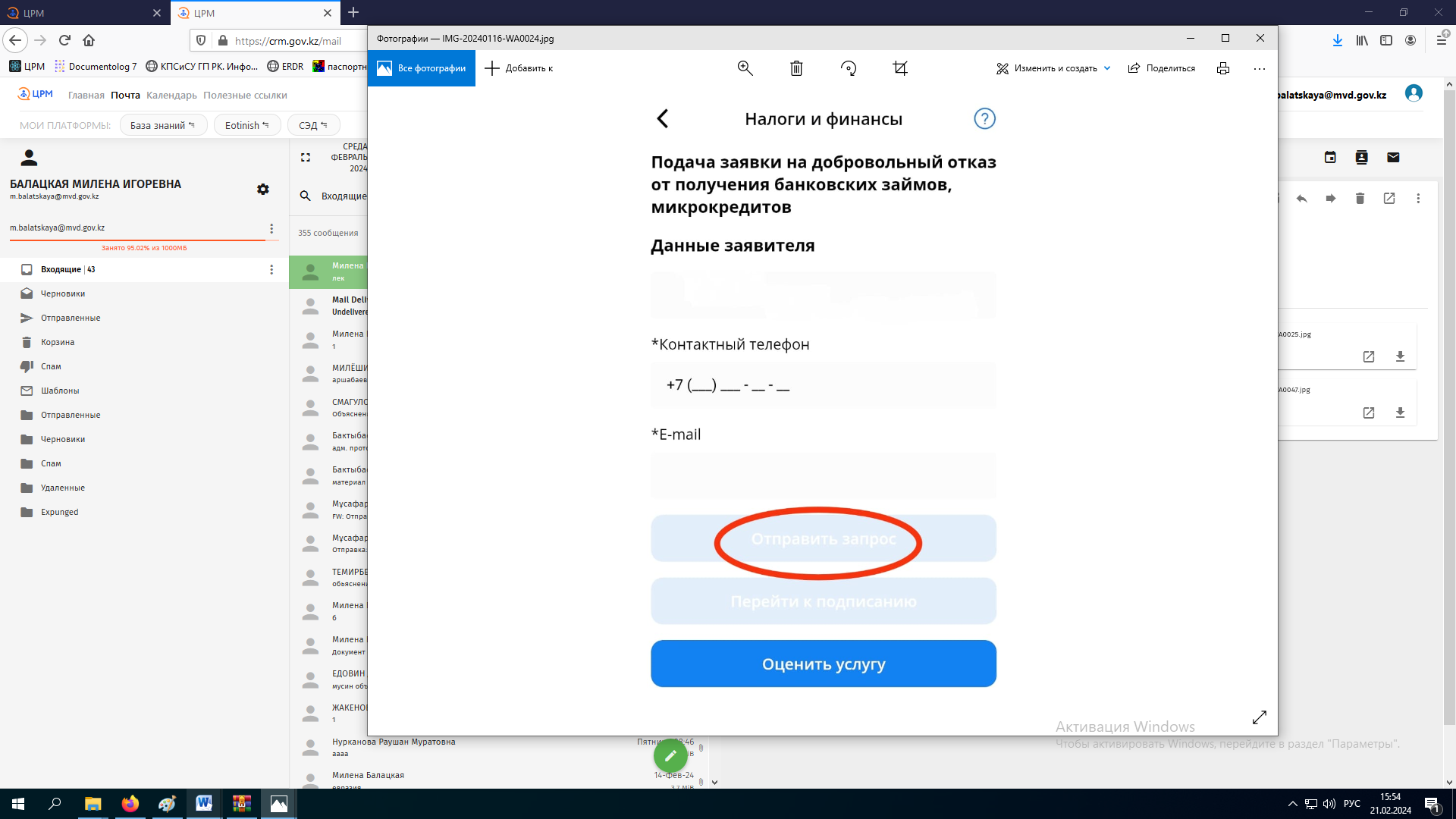
**Не передавайте свои конфиденциальные данные посторонним лицам.**

**Не отвечайте на подозрительные электронные письма или текстовые сообщения от людей, либо организаций, с которыми у вас нет, и не было договорных отношений.**

- очень часто при снятии денежных средств с банкомата или при производстве операций через платежные терминалы граждане оставляют на месте свои квитанции и чеки. Это ни в коем случае нельзя делать, во многих чеках имеются анкетные данные лица, номер сотового телефона, ИИН, сумма последнего перевода/пополнения. Обладая данной информацией мошенник в дальнейшем может Вам позвонить и представиться сотрудником банка, назовет всю полную информацию о Вас и в дальнейшем получить доступ к денежным средствам. После проведения банковских операций чеки и квитанции необходимо сразу уничтожить или забрать с собой, ограничить посторонних лиц от доступа к ним

- если Вам позвонили и представились сотрудником полиции, и сообщили что по вине ваших родственников совершено ДТП, и для не привлечения их к уголовной ответственности нужно внести крупную сумму денежных средств.- Завершите данный телефонный звонок, перезвоните своим близким и убедитесь, что с ними все в порядке.

**- В мобильном приложении EGOV Mobile пользователи могут подать заявку на добровольный отказ от получения кредита, а так же на сайте EGOV. Для этого необходимо в приложении выбрать раздел «Услуги». В разделе «Налоги и финансы» выберете услугу «Добровольный отказ от получения банковских займов, микро кредитов, сроком на 6 месяцев». Укажите свой контактный номер телефона и электронную почту. Нажмите кнопку отправить запрос и подпишите заявку.**

Если человек стал жертвой мошенников, необходимо незамедлительно обратиться в ближайшее отделение полиции, на пульт 102, также подготовить все подтверждающие документы (скриншоты переписок, голосовые сообщения).