МВД РОССИИ
УПРАВЛЕНИЕ
МИНИСТРЕСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО МУРМАНСКОЙ ОБЛАСТИ
(УМВД России по МО)
Управление организации дознания

Ул. Пушкинская, 8А, г. Мурманск, 183038,
тел/факс 815-2 45-79-18

24.09.2021 г. № 10/3616
на № _____ от _____

Об оказании содействия в профилактике преступлений

Исполняющему обязанности
Министра образования и науки
Мурманской области
Т.М. Лариной

ул. Трудовых Резервов, дом 4,
г. Мурманск, 183025

edco@gov-murman.ru

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
НАУКИ МУРМАНСКОЙ ОБЛАСТИ
19 ОКТ 2021
ВХ. № 17/13817

Уважаемая Татьяна Михайловна!

У Управления Министерства внутренних дел Российской Федерации по Мурманской области[1] вызывает озабоченность количество регистрируемых преступлений, совершенных с использованием информационно-телекоммуникационных технологий[2], которое за последние годы неуклонно растет, при этом в первом полугодии 2021 года хоть и удалось сдержать рост указанных преступлений, но кардинально изменить ситуацию не представилось возможным.

Необходимо отметить, что потерпевшими, по указанной категории преступлений, являются граждане, имеющие различные социальный статус, уровень образования, профессиональную занятость и возрастную группу, что бесспорно влияет на эффективность проводимой профилактической работы.

Проведенный Управлением анализ уголовных дел показал, что 95% потерпевших были осведомлены о существующих способах телефонных мошенничеств, однако, не учитывая возможные негативные последствия, в силу личной невнимательности и недостаточной информированности о методах защиты от мошеннических действий, отнеслись к ним безразлично, чем спровоцировали совершение в отношении них преступлений.

---

[1] «Управление Министерства внутренних дел Российской Федерации по Мурманской области» – далее Управление;

[2] «информационно-телекоммуникационные технологии» - преступления, совершенные с использованием сети «Интернет» и средств мобильной связи, включающие в себя, покупки на сайтах клонах, ложные звонки от кредитных учреждений о блокировке карт и счетов, а также сообщения в социальных сетях с просьбами оказания материальный помощи родственникам и знакомым и т.п.

В Мурманской области расположено более 30 подведомственных Министерству образования учреждений общего и профессионального образования, в которых осуществляют трудовую деятельность более 3000 сотрудников и обучаются более 50000 учеников и студентов.

Сотрудники учреждений министерства образования и науки вносят существенный вклад в обеспечение доступности качественного образования всех слоев населения Мурманской области, что требует от них проявления эрудиции и коммуникабельности

Современное общество характеризуется ранней социальной эмансипацией подростков, а развивающиеся телекоммуникационные технологии позволяют им уже в возврате 14 лет быть субъектами рыночных отношений, что накладывает на них дополнительную ответственность. Низкий уровень восприятия и соблюдения мер информационной безопасности наряду с недостаточной финансовой грамотностью подростков делает их особо уязвимыми участниками рыночных отношений.

Исходя из сложившейся обстановки и в целях надлежащего информирования работников образования и их семей, а также повышения уровня финансовой грамотности учащихся 7-11 классов и студентов профильных учебных учреждений просим Вас организовать проведение дополнительных профилактических мероприятий с персоналом учреждений министерства образования и науки Мурманской области, направленных на формирование безопасных механизмов взаимодействия с финансовым миром[3], а также организовать распространение информационно-профилактических материалов среди учащихся 7-11 классов и студентов профильных учебных учреждений.

По нашему мнению, проведение указанных мероприятий позволит сократить число пострадавших от мошеннических действий как работников образования и членов их семей, так и учащихся 7-11 классов, студентов профильных учебных учреждений, что благоприятно отразится на их финансовом благополучии.

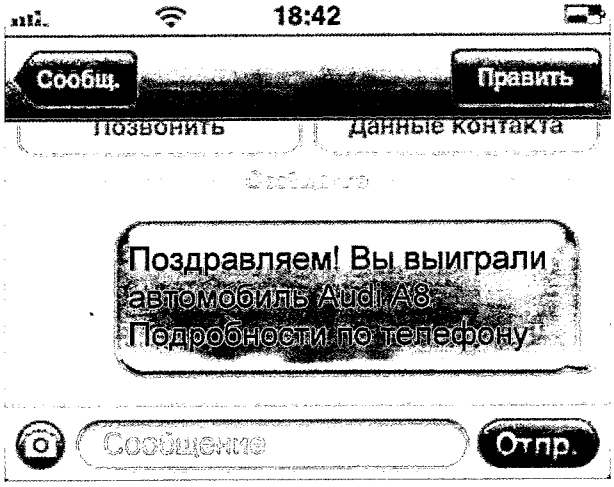
Приложение: информационные листы с правилами поведения, типовыми ситуациями и мошенническими схемами на 13 листах.

С уважением,

Начальник Д.В. Колесников

[3] «формирование безопасных механизмов взаимодействия с финансовым миром» - сохранение и безопасное использование персональных данных, включающих в себя как сведения о банковских счетах, картах, пин-кодах, абонентских номерах, задействованных в системе быстрых платежей, так и сведения о логинах и паролях онлайн сервисов «СБЕР» и «ВТБ», торговых площадок «Авито» и «Юла», а также различных социальных сетей.

СИТУАЦИЯ 1



Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

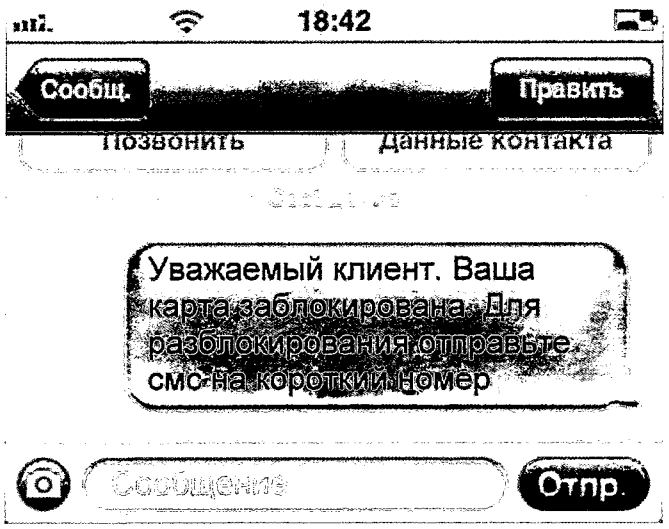
СИТУАЦИЯ 2

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

СИТУАЦИЯ 3



Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

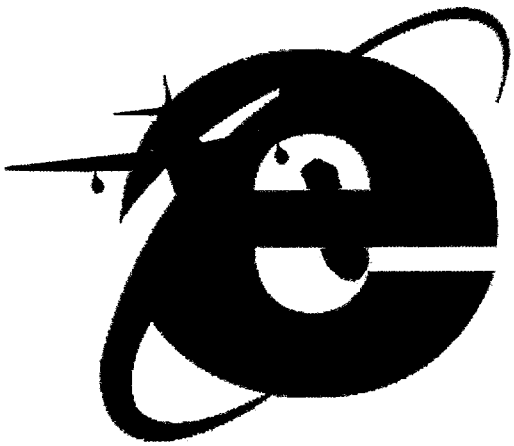
СИТУАЦИЯ 4

На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.

Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.

СИТУАЦИЯ 5

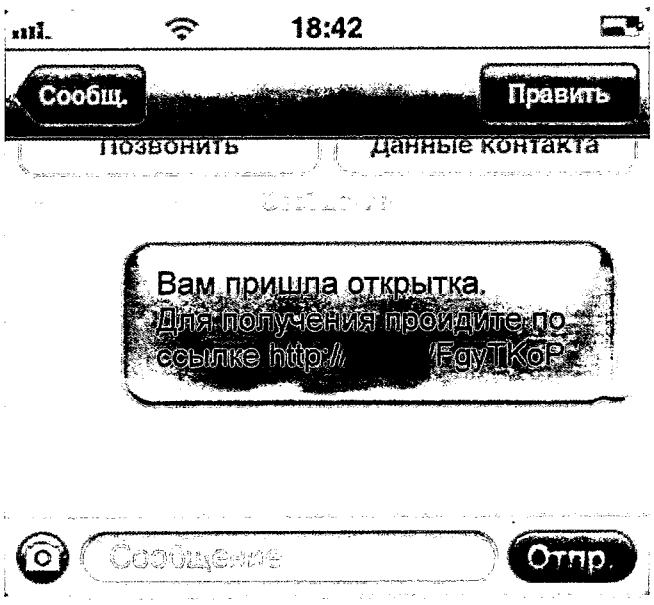


Вы хотите приобрести авиабилеты через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.

Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.

СИТУАЦИЯ 6



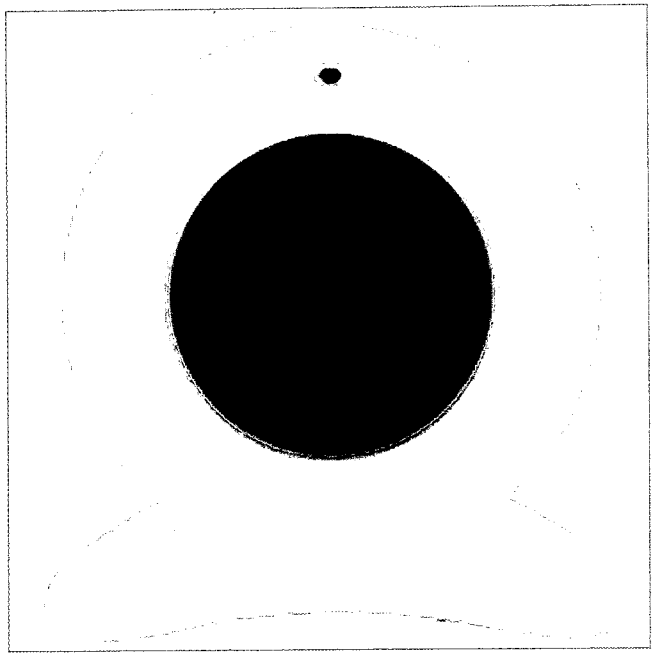
Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

НИКОГДА не переходите по ссылке, указанной в сообщении.

Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

СИТУАЦИЯ 7



Общаетесь в интернете и имеете аккаунты в соцсетях?

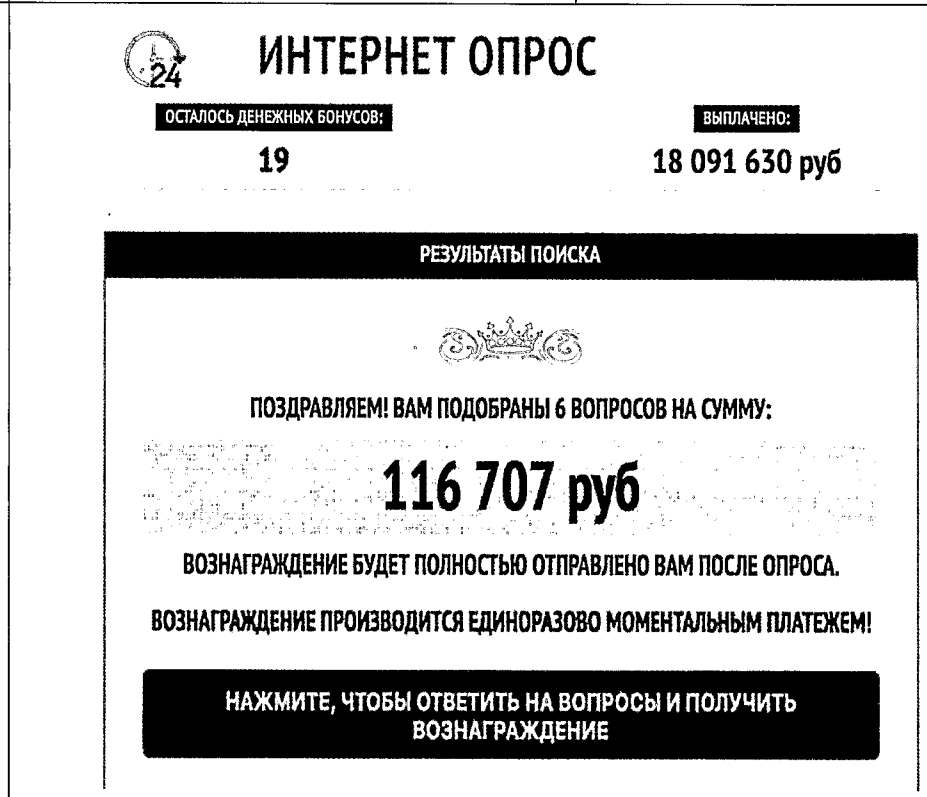
НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

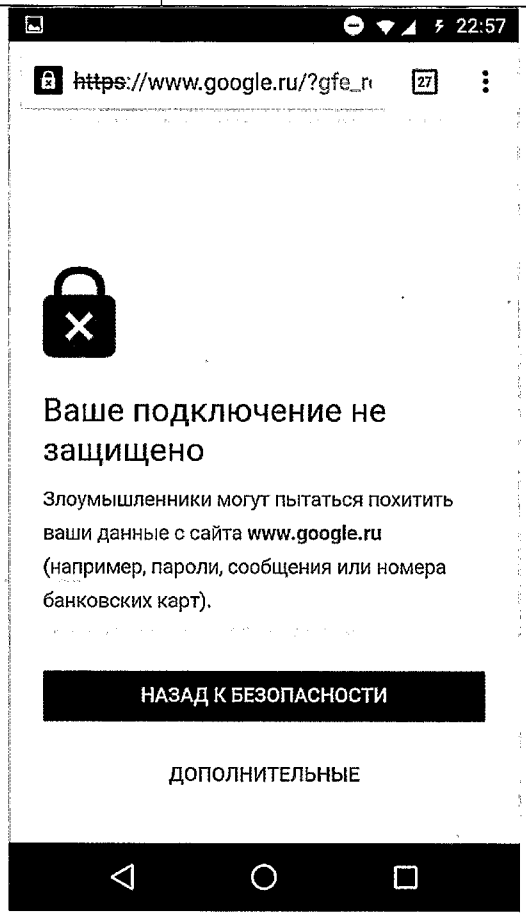
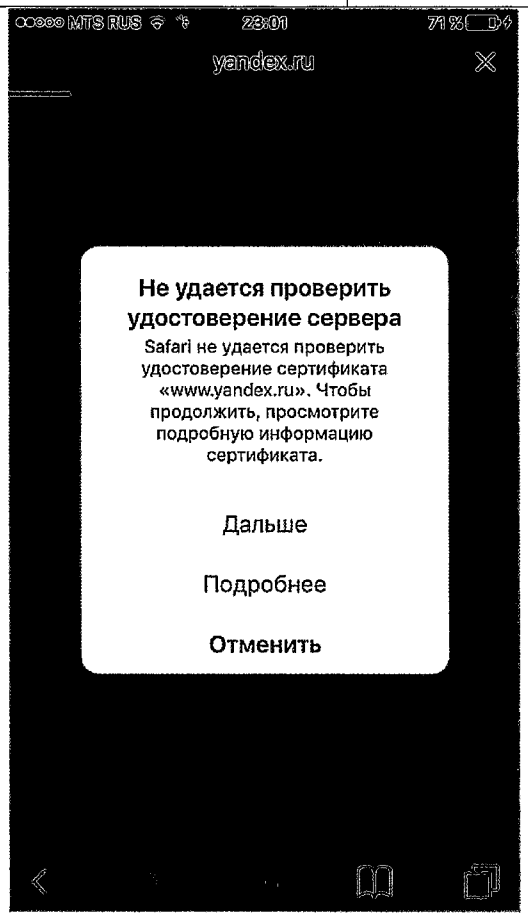
Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

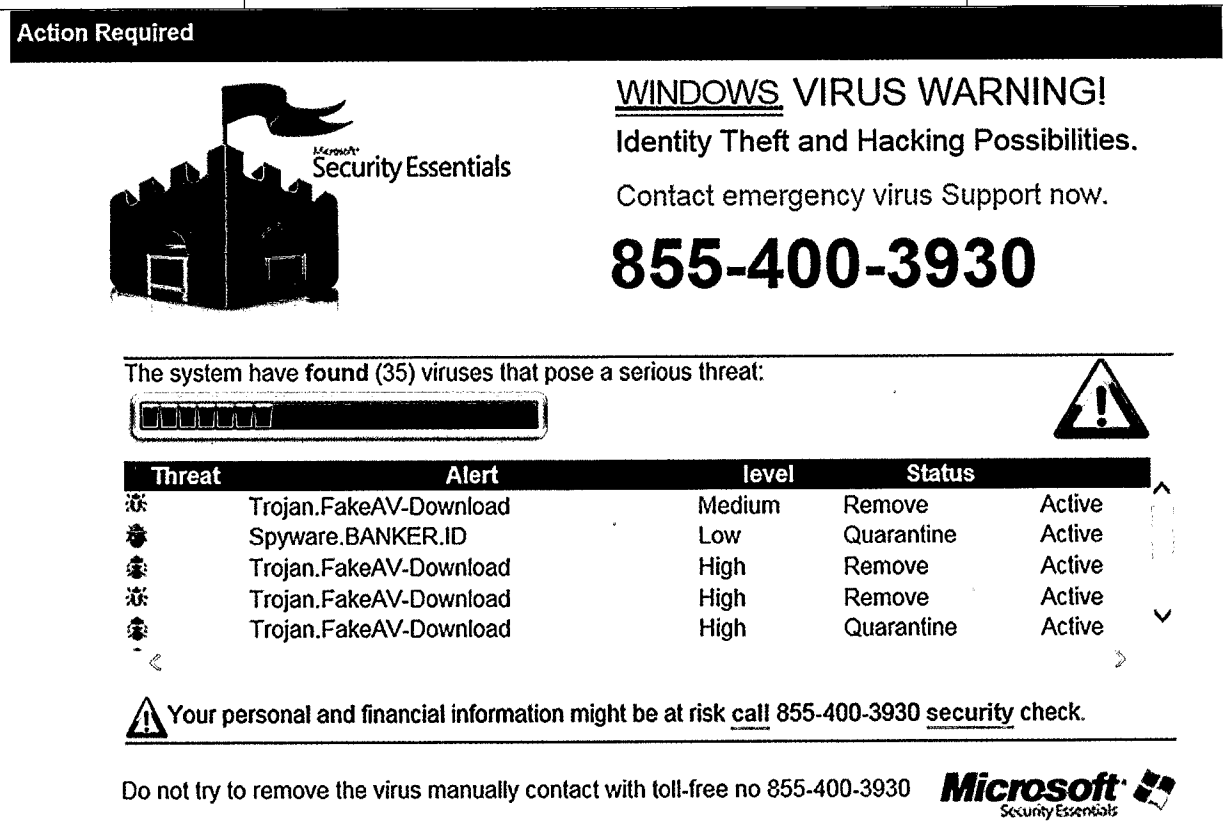
Способы дистанционных мошенничеств.

	Как работает схема	В чем опасность.	Как защититься
Получите деньги за опрос	Мошенники создают сайт, на котором предлагают деньги за простые действия: например, просят пройти короткий опрос или отправить ссылку друзьям. Обещают много: может быть и 200 000 рублей, за ответы на несколько вопросов. Вы отвечаете на вопросы, делитесь ссылкой с друзьями. На последнем шаге выясняется, что нужно «активировать аккаунт», «оплатить комиссию», сделать «закрепительный платеж» или ввести номер карты.	Мошенники возьмут деньги за «комиссию», но никаких выплат не дадут. Реквизиты банковской карты они смогут использовать для будущих списаний. А друзья посчитают вас спамером. Мошенники нередко предлагают получить большие суммы за ответы на 5-10 простых вопросов Для этого нужно всего лишь ввести данные карты, чтобы оплатить небольшую комиссию, например 276 рублей и распрощаться с деньгами	Не стоит верить любой возможности заработка денег за выполнение простых действий, даже если на сайте есть отзывы людей, логотипы известных банков и других авторитетных организаций: все это — уловки мошенников. Если вы ввели данные карты на подозрительном сайте, срочно позвоните в свой банк и расскажите об этом — там подскажут, что делать.

пример



Подключитесь к бесплатному вайфаю	Мошенники создают вайфай-точку, которая не требует пароля и подключиться к интернету может любой желающий. Такое соединение обычно настраивают в людных местах: на улице, в кафе или отеле.	Владелец вайфая видит, на какие сайты заходят все подключившиеся, но это не самое страшное. Он может добраться до паролей, которые вы вводите на этих самых сайтах. Мошенники могут украсть пароли от социальных сетей и почты, а еще реквизиты карты — если вы расплатитесь ею в интернет-магазине. Зная данные карты, мошенники легко выведут деньги на свои счета. А в социальных сетях они увидят сообщения, которые вы никому не хотели показывать, вот и повод для шантажа. Браузер на компьютере и в телефоне сообщит о попытке взлома. Если вы закроете такие предупреждения и продолжите работу, ваши данные смогут украсть мошенники	Убрать в настройках автоматическое подключение к сетям. Не вводить логины и пароли на сайтах с незащищенным соединением или ошибками безопасности. Отключиться от вайфая и работать через мобильную сеть в случаях, когда нужно вводить логин, пароль или данные карты.
пример		 	

Ваш компьютер заражен	Мошенники делают сайт, который сообщает, что с вашим компьютером проблемы. Фразы обычно тревожные: «Ваши данные под угрозой», «Обнаружен вирус», «Срочно защитите компьютер». Чтобы решить эти проблемы, предлагают позвонить на бесплатный номер или написать во встроенный на сайте чат. Во время разговора мошенники убеждают поставить «антивирус» или просят данные банковской карты — чтобы они удаленно почистили компьютер. Посмотреть на Ютубе, как работает эта схема Один такой мошенник недавно заработал 3 миллиона долларов	«Антивирус» оказывается вредоносной программой, которая может заразить компьютер. Доверять удаленное управление компьютером еще опаснее: мошенники могут получить доступ ко всем файлам. Мошеннический сайт, который сообщает о вирусе на компьютере. Просят срочно связаться с поддержкой	Закройте сайт, который рассказывает вам о проблеме. Ничего не скачивайте. Если кажется, что с компьютером действительно что-то не так, обратитесь к системному администратору или специалисту по безопасности, которому доверяете.
пример			

Re:Re: Коллега, у нас проблемы	Мошенник присылает письмо с вложением на рабочую почту. Вложение выглядит как обычный документ, которыми обмениваются через систему электронного документооборота. Но если загрузить и открыть такой документ, то вместо него на компьютер попадет вирус.	Мошенники могут получить доступ к вашему компьютеру, корпоративным системам и интернет-банку и в результате украдут документы и деньги со счета компании. Файлы могут зашифровать и рабочие документы, базы данных и вся переписка станут недоступны. Письмо от мошенников, которое выглядит как обычная рабочая переписка. Внутри документа ссылка на вирус, которая выглядит как кнопка печати.	Внимательно изучите письмо. Должно насторожить обезличенное обращение «добрый день», «коллега» или «сотруднику компании». Перешлите письмо в службу безопасности: если дадут добро скачивайте документ. В противном случае просто отметьте письмо как спам.

пример

Чт 07.02.2019 16:28

Zhdanov <comunicazione@mediatecatoscana.it>

заказ [redacted]

Кому [redacted]

Добрый день!
Отправляю подробности заказа. Документ во вложении и тут: https://www[redacted]/documents/docs/

[redacted] Юрий Рудольфович

Менеджер Департамента по организационному развитию и работе с предприятиями.

ООО [redacted]

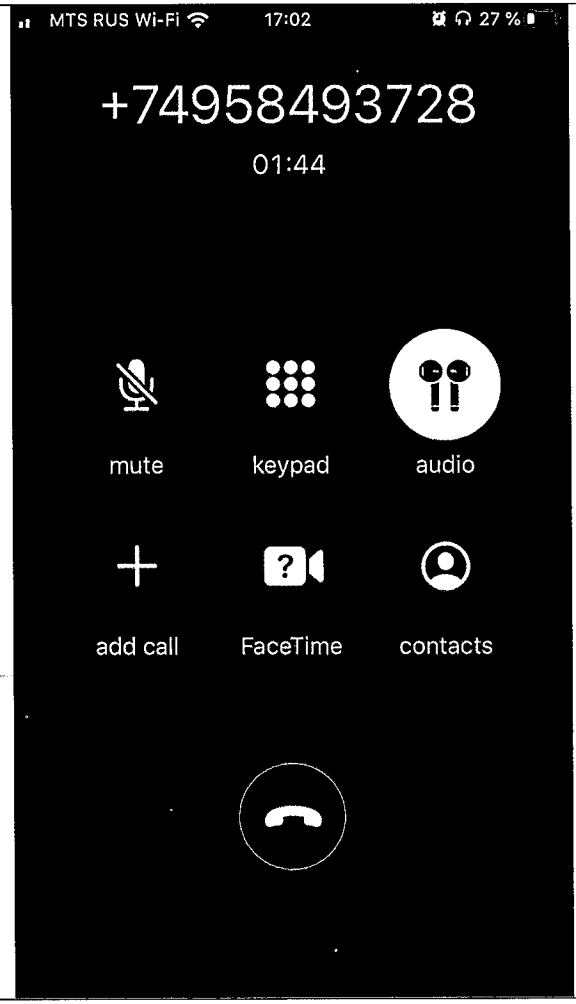
**********Проверено Kaspersky Mail Checker **********

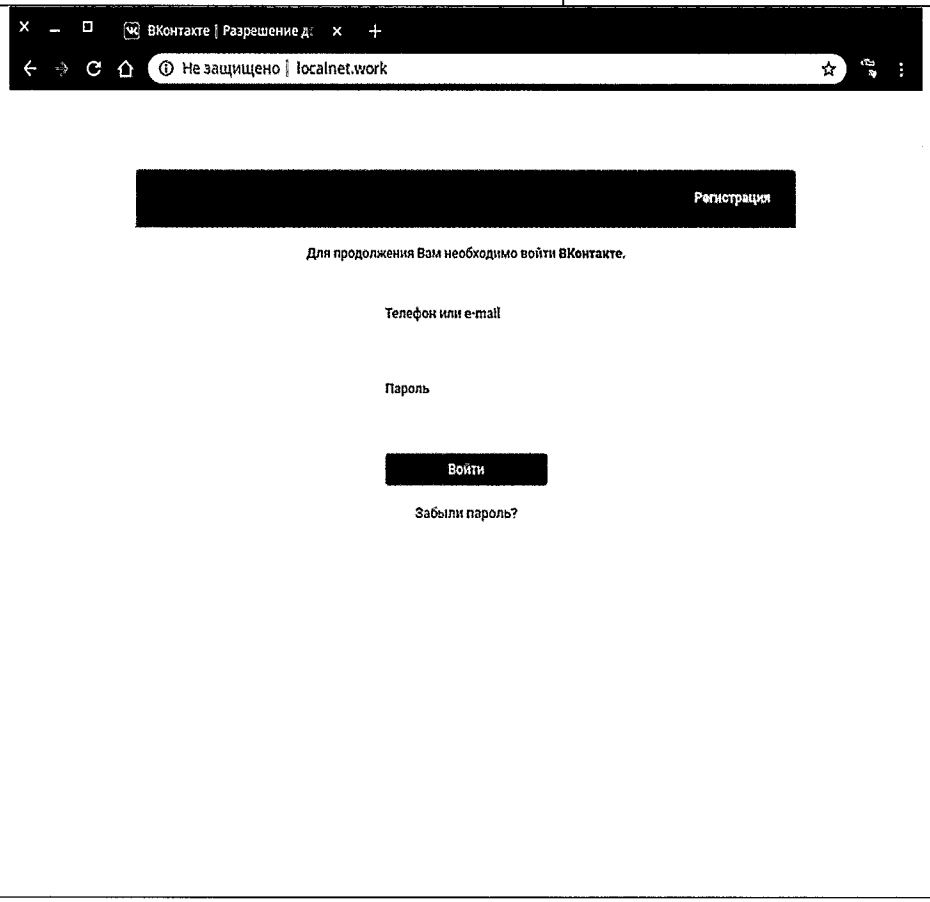
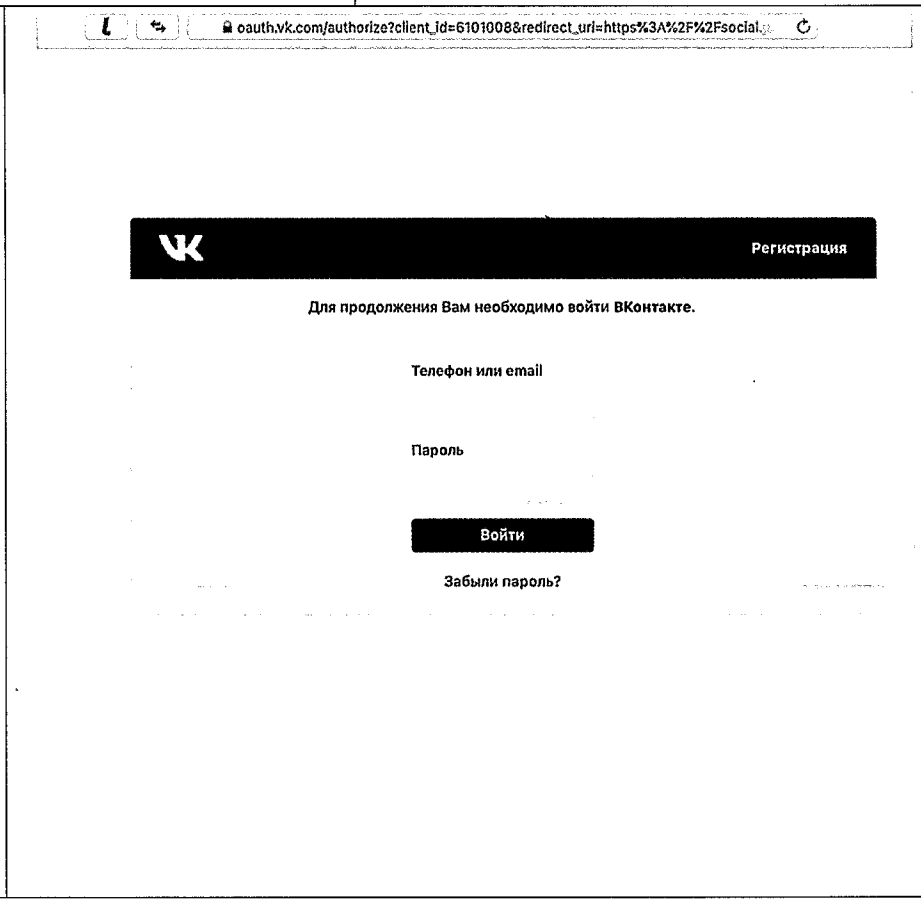
Ваши документы

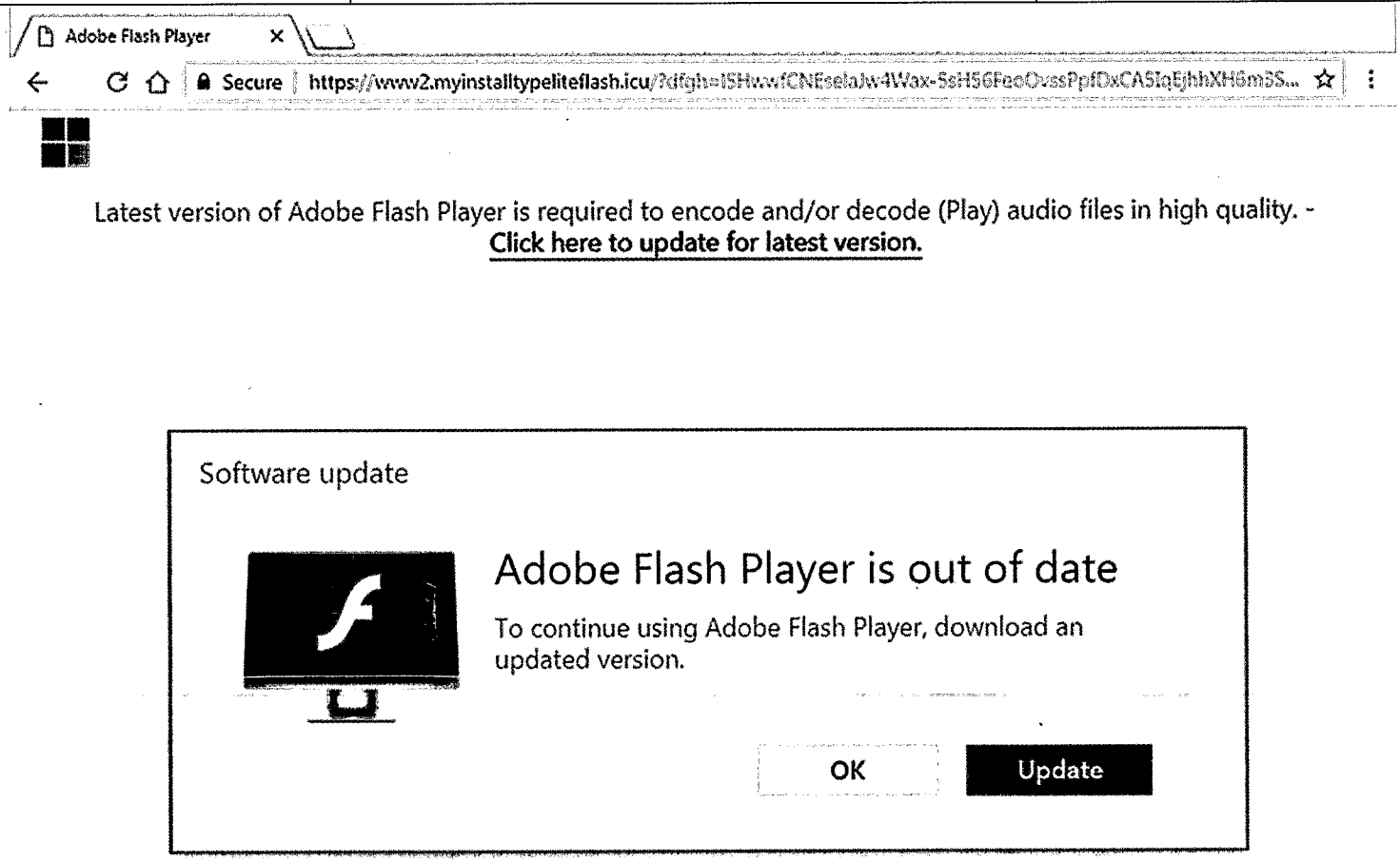
сбис

ЭЛЕКТРОННАЯ ОТЧЕТНОСТЬ И ДОКУМЕНТООБОРОТ

Печать документов на экран

Звонок из банка	Мошенники звонят и представляются сотрудниками банка: говорят, что с вашего счета списаны деньги. Чтобы их вернуть, нужно срочно продиктовать данные карты и сообщить одноразовый код, который придет в смс.	Мошенники получат доступ к вашему интернет-банку и смогут распоряжаться деньгами. Код из смс нужен, чтобы подтвердить перевод на чужую карту или покупку в магазине. В этом случае мошенники даже не потрудились сделать номер «красивым».	Скажите, что не можете говорить, и повесьте трубку. Перезвоните в банк самостоятельно или проверьте счет через мобильное приложение. Если назвали мошенникам код или любые другие данные срочно звоните в банк. Возможно, вы успеете остановить операцию. Запомните: сотрудник банка никогда не попросит назвать код из смс и номер карты при телефонном разговоре.
пример			

Зарегистрируйтесь через Вконтакте	Мошенники делают сайт, например, с бесплатными сериалами, полезными файлами, интересными статьями или стикерами. Для входа или загрузки контента предлагают авторизоваться в социальной сети. Но не на все сайты безопасно заходить через соцсети. Мошенники могут получить ваш пароль таким способом: они сделают так, чтобы сайт не перенаправлял на страницу соцсети, а подсовывал фальшивое окно авторизации. Логотип и оформление будут похожи на настоящие, но это просто копия логин и пароль, введенные в таком окне, останутся на сайте мошенников.	Мошенники получат доступ к вашему аккаунту в социальной сети. И смогут отправлять друзьям спам от вашего имени, читать сообщения и сохранять приватные фотографии. Фальшивое окно авторизации во ВКонтакте. Обратите внимание на адресную строку: соединение не защищено, да и адрес не похож на настоящий. Это настоящее окно авторизации: в адресной строке есть замочек и «vk.com». Логин и пароль отправятся на сервер ВКонтакте, если совпадут — вы зайдете на сайт под учеткой соцсети	Вводите пароли только на тех сайтах, которые открыли сами, например, набрали адрес в браузере или перешли на сайт из «Избранного». Если ввели пароль на подозрительном сайте, как можно скорее зайдите на настоящий и смените его. Включите двухфакторную аутентификацию в почте, социальных сетях и мессенджерах. Тогда кроме логина и пароля потребуется что-то еще: например, код из специального приложения или смс. Мошенники не смогут зайти в ваш аккаунт, даже если украдут или подберут пароль.
пример			

Срочно обновите программу	Любая программа на компьютере или смартфоне рано или поздно попросит обновлений. Это нормально, и чаще всего обновления полезны. Другое дело, когда обновить программу неожиданно предлагает сайт. Вы скачиваете «обновление» для флеш-плеера, браузера, антивируса или операционной системы, но оно оказывается вирусом.	Фальшивое обновление дает мошенникам доступ к вашему компьютеру, паролям, аккаунтам в социальных сетях. А еще оно может зашифровать файлы и предоставить удаленный доступ к компьютеру. Мошеннический сайт предлагает установить вирус под видом легальной программы — обновления для флеш-плеера	Закройте сайт, на котором предлагают установить обновление. Если нужно обновить операционную систему, браузер или приложение — сделайте это самостоятельно на официальных сайтах, или обратитесь к системному администратору, которому доверяете.
пример			

Обнаружен вход с незнакомого устройства	На почту приходит письмо якобы от службы безопасности Гугла. Пишут, что в ваш аккаунт заходили с неизвестного устройства, и просят проверить настройки безопасности. Для этого нужно попасть в профиль — ссылку для входа заботливо прикладывают. По ссылке действительно появляется привычное окно авторизации в гугл-аккаунте, и жертва вводит логин и пароль. Фишка в том, что ссылка ведет на гугл-переводчик, а новое окно с привычной формой входа — это просто перевод фишинговой страницы. Тем не менее окно активно и в него можно ввести логин и пароль. За этими данными и охотятся мошенники.	Все, что хранится на гугл-диске, получат мошенники: письма, доступ к другим сайтам и даже данные о ваших перемещениях. Так выглядит фишинговая страница, которую прогнали через гугл-переводчик. На первый взгляд, все легально: в адресной строке — адрес translate.google.com, который кажется доверенным, а окно входа в аккаунт не выглядит подозрительно. Настоящий адрес мошеннического сайта написан в поле поиска ниже, но туда уже мало кто смотрит	Проверьте, на каких устройствах выполнен вход в аккаунт. Настройте двухэтапную аутентификацию. Скачайте на смартфон приложение, которое генерирует одноразовые пароли. Если мошенники успели изменить пароль, восстановите гугл-аккаунт.
пример			

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

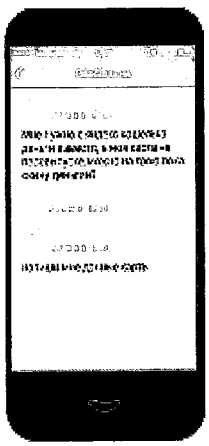
ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



СООБЩЕНИЯ ОТ ДРУЗЕЙ

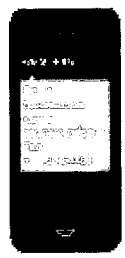
Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!



БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША
(компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.