



**МИНИСТЕРСТВО  
ОБРАЗОВАНИЯ, НАУКИ  
И МОЛОДЕЖНОЙ ПОЛИТИКИ  
КРАСНОДАРСКОГО КРАЯ**

Рапшилевская ул., д. 23, г. Краснодар, 350063  
Тел. (861) 298-25-73, (861) 298-26-00  
E-mail: minobrkruban@krasnodar.ru

15.11.2012 № 47-01 В-2012/26/22

На № \_\_\_\_\_ от \_\_\_\_\_

Руководителям органов местного самоуправления муниципальных образований Краснодарского края, осуществляющих управление в сфере образования и молодежной политики

Об использовании материалов

Уважаемые коллеги!

Направляем для использования в работе по профилактике киберпреступности тематические материалы, подготовленные Министерством внутренних дел Российской Федерации.

Приложение: на 22 л. в 1 экз.

Заместитель министра

С.Е. Урайкин

Юдина Татьяна Олеговна  
+7 (861) 298-25-70



**Министерство внутренних дел Российской Федерации**

**ТЕМАТИЧЕСКИЕ МАТЕРИАЛЫ**  
**по противодействию IT-преступлениям**  
**(для использования при проведении правовой**  
**и информационно-разъяснительной работы с гражданами)**

**Москва – 2022**

С внедрением в повседневную жизнь телекоммуникационных сетей и новых технологий стала активно применяться дистанционная система обслуживания граждан: предоставление государственных услуг в электронном виде, выдача паспортов, медицинских карт и другие. Данные нововведения, с одной стороны, облегчили обмен полезной и значимой информацией, доступ клиентов к различным услугам и операциям, а с другой – стали использоваться в преступной деятельности.

Злоумышленники используют весь возможный арсенал средств, чтобы сохранить свою анонимность и остаться безнаказанными. Мошенники действуют в максимально короткие сроки, входят в доверие и совершают преступления в течение нескольких минут.

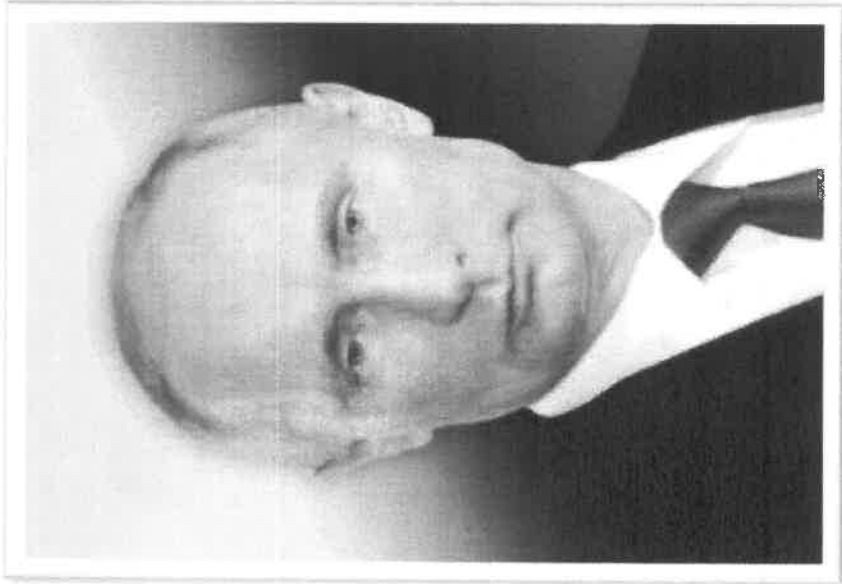
Сложившиеся в мире обстоятельства социально-экономического характера, вызванные пандемией коронавируса COVID-19, создали дополнительные условия для усиления криминальной активности в интернет-пространстве.

В целях противодействия правонарушениям рассматриваемой категории Министерством внутренних дел Российской Федерации принимаются активные меры по развитию ведомственной нормативной правовой базы, методик раскрытия и расследования конкретных видов IT-преступлений, повышению уровня профессиональной подготовки сотрудников оперативных подразделений, экспертов, следователей и дознавателей, а также техническому оснащению профильных подразделений полиции.

Практический опыт деятельности подразделений органов внутренних дел Российской Федерации показывает, что одним из наиболее эффективных методов противодействия киберпреступлениям является информирование населения о новых способах, схемах их совершения и методах защиты от них.

Важность этой работы подчеркнул в своём выступлении на расширенном заседании коллегии МВД России по подведению итогов оперативно-служебной деятельности органов внутренних дел за 2021 год Президент Российской Федерации В.В. Путин.

Тема противодействия преступлениям данного вида неоднократно обсуждалась на совещаниях руководителей правоохранительных органов, в том числе на международном уровне.



«...Нужна последовательная, более результативная работа по всем видам преступлений, которые представляют угрозу для нашего общества. В том числе речь идёт о новых вызовах, связанных с проникновением криминала в сферу информационных технологий и телекоммуникаций. Количество преступлений в этой сфере ежегодно растёт. В результате действий кибермошенников урон несут отечественные компании. И, что вызывает особую остроту общественной реакции, с потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане во всё большем и большем количестве. Жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью. У преступников нет ничего святого, только бы деньги урвать...»

Президент Российской Федерации Владимир Путин



Из выступления  
на расширенном заседании  
коллегии МВД России  
по подведению итогов  
оперативно-служебной  
деятельности органов  
внутренних дел за 2021 год  
17.02.2022

«В Российской Федерации с использованием IT-технологий по-прежнему совершается каждое четвертое преступление. Однако за три месяца текущего года\* их количество заметно сократилось – на 8,5%. По мнению специалистов, это свидетельствует о том, что в данном процессе были массово задействованы кол-центры, расположенные на Украине и обезвреженные в ходе специальной военной операции Вооружённых Сил Российской Федерации».

Министр внутренних дел Российской Федерации  
генерал полиции Российской Федерации  
**Владимир Колокольцев**

\* За период с января по март 2022 года



Из выступления  
на Совещании министров  
внутренних дел  
и общественной безопасности  
государств – членов ШОС  
18.08.2022



# ОСНОВНЫЕ ВИДЫ ДИСТАНЦИОННЫХ ХИЩЕНИЙ

## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Самым «действенным» способом мошенничества остаётся социальная инженерия – обман на доверии. Суть социальной инженерии состоит в том, что злоумышленник вводит в заблуждение жертву и та выполняет его инструкции, сама отдаёт ему деньги либо пароль от личного кабинета в онлайн-банке.

### Социальная инженерия

Данный термин придуман ещё в начале 2000-х годов бывшим компьютерным хакером, признанным виновным в совершении различных компьютерных и коммуникационных преступлений, утверждавшим, что самое уязвимое место в кибербезопасности – человек.

Надо отметить, что характерной чертой современных правонарушителей является беспринципность действий. Мошенники с помощью психологического манипулирования заставляют людей делать то, что они делать не собирались, обманным путём выманивая у них последние сбережения, заставляя брать на себя кабальные кредитные обязательства.

Ключевым фактором, способствовавшим совершению указанных преступлений, является низкий уровень правовой и финансовой грамотности населения.



## МВД РОССИИ ПРЕДУПРЕЖДАЕТ

Будьте бдительны! Звоните 02 или 102

**НЕ ОТКРЫВАЙТЕ ДВЕРЬ НЕЗНАКОМЫМ** людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, коммунальщиков, ЖКХ и т.д. Позвоните в управление, направивши им в Ваш адрес специальную



### НЕ ДОВЕРЯЙТЕ

если Вам звонят и сообщают, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести деньги, штраф, а также купить дорогие лекарства – в общем откупиться. **ЭТО НЕМАМ!**

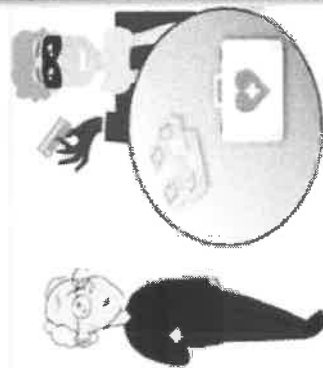


### СЛЕДИТЕ ЗА СОБРАНОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ

Абсурдны рассказы о том, что Вам толкуют, чтобы выдать или вернуть, а чтобы их получить, надо подписать ряд документов. А вместо этого под давлением наложить доверенность или дарственную на Вашу квартиру!



Не подписывайте никакие документы!



Мошенники сообщают о выигрыше, предлагают банковскую карту, о переводе заработной платы, срочном обмене денег на деньги или предлагают приобрести товары и таблетки по низким ценам. **НЕ ВЕРЬТЕ – ЭТО МОШЕННИЧЕСТВО!**

## ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

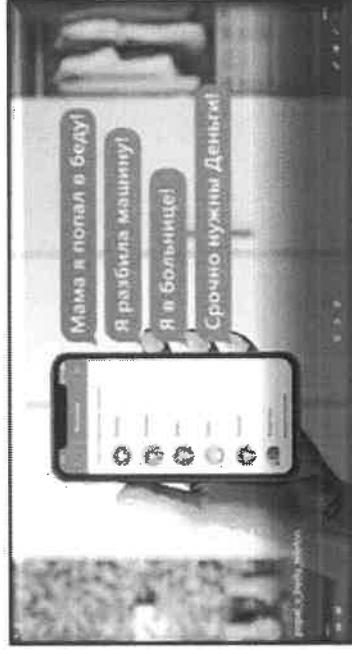
**Обман по телефону: «Меня задержали, но можно откупиться»**

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном заявляет, что уже не раз помогал людям таким образом. Для решения вопроса необходима определённая сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.

**Шокунул сомнительный звонок? Вам необходимо:**

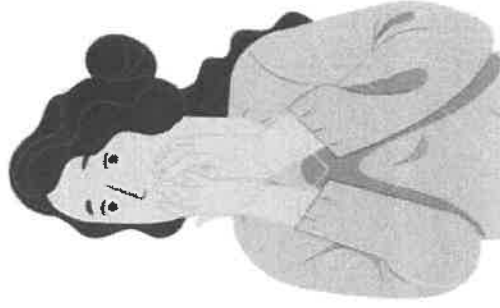
- прервать разговор и перезвонить тому, о ком идёт речь;
- если телефон отключён, связаться с его друзьями и родственниками для уточнения информации;
- если разговор происходит якобы с представителем правоохранительных органов, узнать, из какого он подразделения;
- набрав 02 и уточнить в дежурной части названного Вам подразделения, действительно ли родственник тула доставлен.



## SMS, сообщения — просьба о помощи



Абонент получает сообщение на мобильный телефон: «У меня проблемы, кинь денег на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.



Пожилым людям, детям и подросткам следует объяснить, что на сообщения с неизвестных номеров реагировать нельзя, это могут быть мошенники!

## Телефонный номер-грабитель

Вам приходит сообщение с предложением перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной — помощь другу, проблемы со связью или с Вашей банковской картой и другие.

После набора номера Вас долго держат на линии. Когда это надоедает, Вы отключаетесь — и оказывается, что с Вашего счёта списаны крупные суммы.

## НА САМОМ ДЕЛЕ:

Мошенники регистрируют сервис с платным звонком без предупреждения абонента о снятии платы за звонок.

Будьте бдительны, совершая звонок по чужой просьбе!

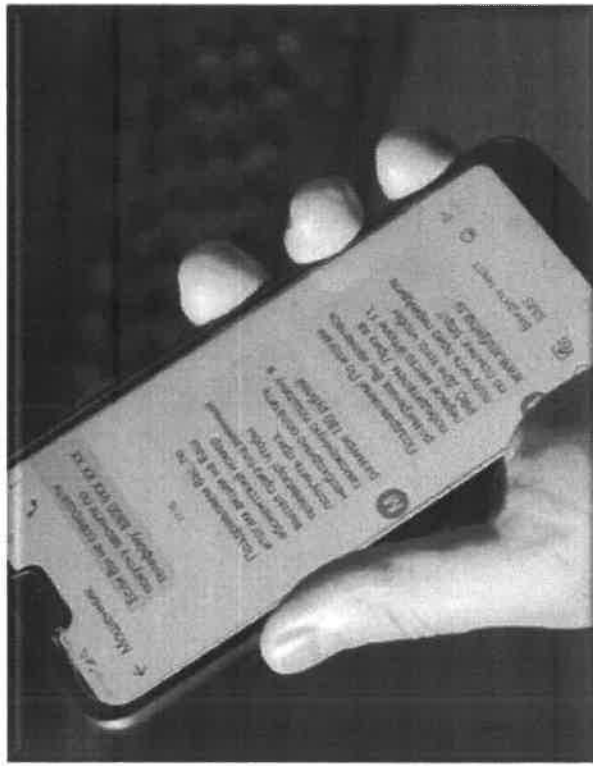
**Единственный способ обезопасить себя от телефонных мошенников — это не звонить по неизвестным номерам!**



### «Выигрыш» в лотерею

Мошенники направляют сообщения с неизвестных номеров о выигрыше с просьбой осуществить перевод денежных средств для его получения либо вернуть якобы направленные (переведённые) ошибочно Вам денежные средства.

Если раньше мошенники звонили людям по телефону и рассказывали о выигрыше в лотерею, потом посылали такую информацию в SMS или по электронной почте, то сейчас им достаточно создать группу в социальной сети или мессенджере – «клиенты» придут сами.



Необходимо помнить, что человек не может выиграть приз, не участвуя в лотереях, родственники не будут отправлять сообщения с неизвестных номеров. Это обман. В этой связи не стоит отвечать на данные сообщения, а тем более отправлять информацию о своей банковской карте и переводить денежные средства!

### «Ошибочный» перевод средств

Вам приходит SMS-сообщение о поступлении средств на счёт, переведённых с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг. Сразу после этого поступает звонок, и Вам сообщают, что на Ваш счёт ошибочно переведены деньги, и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.


Если Вас просят перевести якобы ошибочно переведённую сумму, посоветуйте с чеком о проведённой операции обратиться в отделение банка.

Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

### Деньги за онлайн-опрос

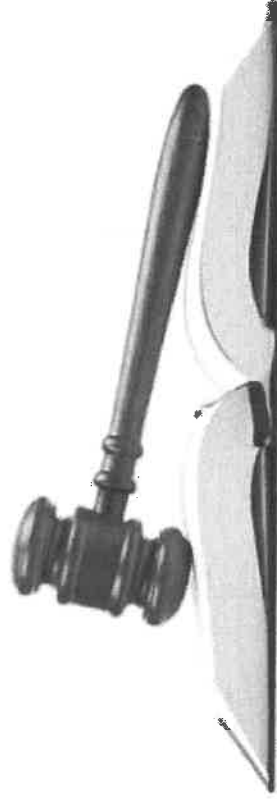
Мошенники предлагают ответить на несколько простых вопросов в Интернете, обещая выплатить баснословные деньги. Однако, чтобы их получить, нужно заплатить «комиссию». Естественно, после этого никакие деньги участнику опроса не приходят.

**Платные  
Опросы**



*Тут за ответы платят деньги!*

### Юридическая Консультация БЕСПЛАТНО



### Бесплатный адвокат

Мошенники звонят гражданам и сообщают, что они стали потерпевшими по уголовному делу и им полагается адвокат. Его услуги якобы бесплатны, но нужно заплатить «госпошлину» — несколько тысяч рублей. Следует иметь в виду, что законом это не предусмотрено.

Если Вам предлагают просто так что-то очень выгодное, то, скорее всего, это обман. Не нужно верить таким предложениям.

## Компенсация от «Минздрава России»

Мошенники в социальных сетях рассылают фейковую информацию, в которой сообщают гражданам, что им положены социальные выплаты, например, компенсация расходов на лекарства, а дальше предлагают пройти по указанной ссылке.

Зачастую злоумышленники пишут от первого лица: «Да, действительно вышел новый закон, я на себе проверил!» В доказательство прикладывают скриншоты с переводом денег от «Сбербанка». Их цель, чтобы человек перешёл по ссылке на сайт, в названии которого иногда даже используется слово «Минздрав», и ввёл свои персональные данные.



## Компенсация от «Минфина России»

Обычно таким образом обманывают потерпевших от преступлений. Им звонят и говорят, что правительством выделена значительная компенсация для тех, кто пострадал от финансовых пирамид и других мошенничеств. Но, чтобы получить деньги, нужно якобы заплатить 1% от суммы компенсации.

Необходимо помнить, что мошенники рассылают подобные фейковые сообщения от различных государственных органов. Не поддавайтесь на их уловки!

## МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определённый номер для получения подробной информации. Когда Вы это делаете, Вас просят сообщить номер карты, СВС-код или ПИН-код для её перерегистрации.

Для того чтобы ограбить Вас, злоумышленникам нужны лишь реквизиты Вашей карты. Получив их, мошенники незамедлительно снимут деньги с Вашего счёта!

ЗЛОУМЫШЛЕННИКОВ ИНТЕРЕСУЮТ РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ, ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБОРОТЕ, А ТАКЖЕ КОДЫ ПОДТВЕРЖДЕНИЯ

ИЗ SMS-СООБЩЕНИЙ.



Необходимо помнить, что ни одна организация, включая банк, не вправе требовать Вашего СВС-код (трёхзначный код) или ПИН-код. Для того чтобы проверить достоверность информации о блокировке карты, следует самим позвонить в клиентскую службу поддержки банка (её телефон указан на оборотной стороне карты). Скорее всего, специалисты ответят, что Ваша карта продолжает обслуживаться банком.

## ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ОБРАЩЕНИИ С БАНКОВСКИМИ КАРТАМИ

### Нельзя:

- хранить ПИН-код рядом с картой, записывать его на бумаге;
- прибегать к помощи третьих лиц при проведении операций с банковской картой в банкоматах;
- позволять посторонним лицам использовать Вашу пластиковую карту.

## ФИШИНГ

Вид интернет-мошенничества, цель которого – получить Ваши персональные данные, получил название **фишинг** (от англ. fishing – рыбная ловля, выуживание).

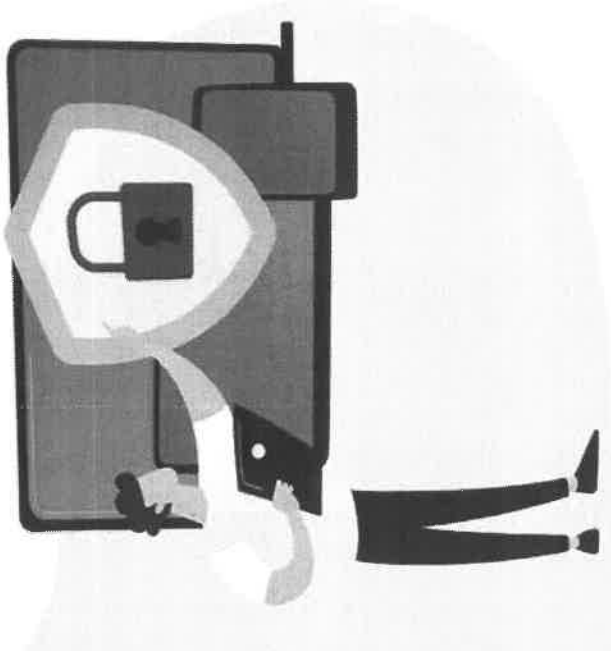
Злоумышленники рассылают электронные письма от имени банков, платёжных систем, маркетплейсов и сервисов. Пользователю предлагается зайти на интернет-ресурс – точную копию настоящего сайта организации, которой человек склонен доверять.

Для дальнейшей возможности использовать своего пластиковую карту Вас просят указать её СVC-код и другие данные. Впоследствии эти данные используются для хищения денежных средств, содержащихся на Вашем счёте.

Фишинг используется мошенниками также на сайтах знакомств, поиска работы, консультационных услуг и т.д.

### Следует помнить:

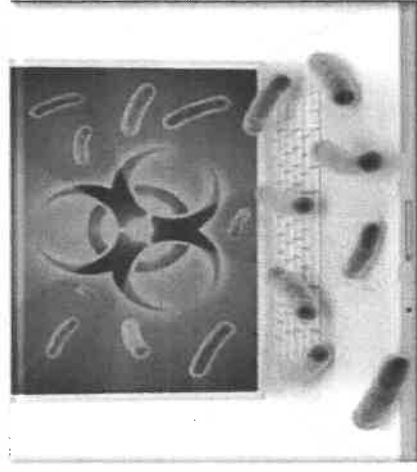
- банки и платёжные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой о предоставлении своих данных;
- сотрудники банка располагают достаточной информацией о своих клиентах;
- сотрудники банка могут у Вас спросить кодовое слово в том случае, если Вы им сами позвонили.



Если звонят «из банка», то попросите «сотрудника» набрать Вам через пять минут. Прервав разговор с незнакомцем, позвоните сами в свой банк по номеру, который указан на Вашей карте, и поговорите с реальной службой поддержки банка.

## ВРЕДОНОСНЫЕ ПРОГРАММЫ И ТАКТИКА БОРЬБЫ С НИМИ

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и распространяют вредоносные программы.



**Вредоносные программы** – любое программное обеспечение, которое предназначено для скрытного (несанкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом «вирусы». Их можно разделить на три группы: компьютерные вирусы, сетевые черви, троянские программы.

## ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

- установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы;
- регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы; пользовательское программное обеспечение для работы в сети, такое как интернет-браузеры, почтовые программы;
- не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников – скачанные с неизвестных веб-сайтов, присланные по электронной почте;
- по возможности не сохраняйте в системе пароли и периодически меняйте их.

## РАБОТА ПО ПРОФИЛАКТИКЕ КИБЕРПРЕСТУПЛЕНИЙ

Министерством внутренних дел Российской Федерации ведётся работа по поиску и разработке новых форматов профилактического воздействия на граждан с целью предупреждения максимально широких слоев населения о новых схемах мошенничества. Решающее значение при выборе форматов профилактики имеют социально-демографические характеристики целевой аудитории. При проведении профилактических мероприятий с аудиторией старшего возраста в качестве основных каналов получения сведений о происходящих событиях предпочтение отдаётся теле- и радиопрограммам, а также наглядной агитации. А при работе с молодёжью большее внимание уделяется мультимедийному контенту в интернет-ресурсах.



Реализуется информационный проект «Предупреждён – значит, вооружён!», в рамках которого в различных форматах рассказывается о преступлениях, совершаемых с использованием высоких технологий, конкретных примерах и методах профилактики кибермошенничества.

Старт проекту дала официальный представитель МВД России Ирина Волк, записав видеобращение с рассказом об основных методах работы аферистов, использующих IT-технологии, а также с рекомендациями, как не стать жертвой обмана.

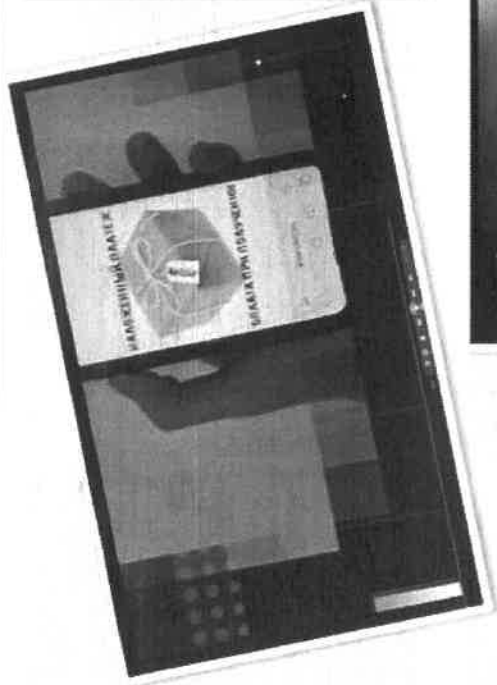
Тематические мультимедийные материалы доступны в социальных сетях под хештегами:

**#ПредупрежденЗнаютВооружен** **#ПредупрежденИВооружен**

На информационном интернет-портале «МВД МЕДИА» и официальном сайте МВД России в тематическом разделе «Внимание, мошенники!» размещена серия профилактических роликов под общим названием «МВД России предупреждает: осторожно, мошенники!».

Видеоролики также опубликованы в тематическом плейлисте канала МВД России в видеохостингах Rutube, VK Видео, YouTube.

**«МВД России предупреждает!» – серия видеороликов**



В телеграм-канале «МВД МЕДИА» опубликована серия профилактических видеороликов, подготовленных МВД России, в которых даны разъяснения, как распознать мошенника, избежать потери денежных средств.



Плейлист с профилактическими видеороликами





Тематические материалы, подготовленные в рамках проекта «Предупрежден — значит, вооружен!»  
(рекомендуются для распространения в социальных сетях)

**К вам обратился  
через соцсети  
старый приятель  
с просьбой одолжить  
пару тысяч?**



**Вполне вероятно,  
что это мошенник!**

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

#ПредупрежденЗначитВооружен  
#ПредупрежденИВооружен



**Некоторые граждане  
осуществляют необдуманные  
финансовые операции  
и переводят деньги на  
указанные им номера  
и счета, в результате чего  
становятся  
жертвами мошенников**



ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**Злоумышленник может  
получить доступ к странице  
вашего друга  
и от его имени просит:**

- занять денег
- предоставить реквизиты  
банковских карт
- перейти по сомнительной  
ссылке



ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**Не поленитесь  
перепроверить информацию,  
позвонив  
дорогому вам человеку,  
чтобы убедиться  
в необходимости  
осуществления финансовой  
операции.**



Скажите знакомым,  
что вы уже вооружены!

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

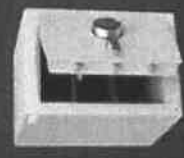
ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**Телефонные мошенники  
стали применять  
новый способ  
психологического  
воздействия  
на клиентов банков**



ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**Получая обманным путем  
персональные данные,  
данные платежных карт,  
информацию  
о совершенных  
по ним операциях  
и другие сведения,  
аферисты используют  
их для хищения  
сбережений  
со счетов  
граждан**



**#ПредупрежденЗначитВооружен  
#ПредупрежденИВооружен**



ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**Злоумышленники  
представляют сотрудникам  
МВД России**



**или других правоохранительных  
органов и сообщают,  
что в отношении собеседника  
возбуждено уголовное дело  
по заявлению представителей  
банка России**

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

**МВД России разъясняет:**

**в случае возбуждения уголовного  
дела в отношении гражданина  
на почтовый адрес по месту  
его проживания официально  
направляется повестка о вызове  
в отдел полиции к следователю  
или дознавателю**



**Повестка может быть направлена как  
в рамках возбужденного уголовного дела,  
так и в рамках доследственной проверки,  
проведения иных процессуальных действий.**

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

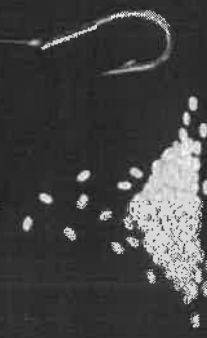
Уважаемые граждане!  
Остерегайтесь различных  
сомнительных  
инвестиционных проектов,  
брокерских организаций.



Не спешите перечислять  
все имеющиеся  
денежные средства  
посторонним лицам.

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

Сначала вы получаете  
прибыль, это затягивает.



Затем ситуация меняется  
и вы проигрываете все.  
Но «наставник» предлагает  
взять кредит и отыграться.  
Далее все повторяется....

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

Вам обещают доход  
от 20% годовых до бесконечности?

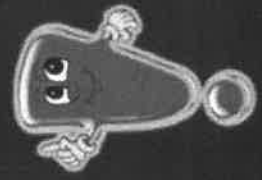
Чтобы торговать на валютном рынке,  
мошенник предлагает  
вам заключить договор.



Он отправит вас  
на подставной сайт  
и деньги, которые вы переведёте,  
попадут к нему,  
а не на брокерский счёт.

ПРЕДУПРЕЖДЕН - ЗНАЧИТ ВООРУЖЕН

Проявляйте в общении  
с незнакомцами  
бдительность  
и осторожность!



#ПредупрежденЗначитВооружен  
#ПредупрежденИВооружен



#ПРАВОВАЯСПРАВКА

МВД России

# Правила цифровой гигиены в условиях удаленной работы

www.grouper-ib.ru

**Правила цифровой гигиены в условиях удаленной работы**



## ЛИЧНОЕ И РАБОЧЕЕ

По возможности работайте на корпоративном компьютере. Не загружайте и не открывайте корпоративные файлы на личные устройствах.

**Правила цифровой гигиены в условиях удаленной работы**



## РАЗРЕШЕННЫЕ КАНАЛЫ СВЯЗИ

Если использование определенных мессенджеров ранее не было разрешено корпоративным регламентом, не начинайте их использование сейчас.

grouper-ib

# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ



## НАСТРОЙКА УДАЛЕННОГО ДОСТУПА

Заранее позаботьтесь о получении удаленного доступа к необходимым ресурсам и следуйте указаниям ИТ-специалистов для его настройки.



## ЛИЧНОЕ И РАБОЧЕЕ

По возможности работайте на корпоративном компьютере. Не загружайте и не открывайте корпоративные файлы на личных устройствах.



## РАЗРЕШЕННЫЕ КАНАЛЫ СВЯЗИ

Если использование определенных мессенджеров ранее не было разрешено корпоративным регламентом, не начинайте их использование сейчас.



## ВНИМАТЕЛЬНОСТЬ

Домашняя сеть не защищается отделом ИБ, поэтому будьте внимательны — атаковщики могут воспользоваться ситуацией и направить усилия на менее защищенные устройства.



## ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Проверьте, настроена ли двухфакторная аутентификация в почте, в мессенджерах и при VPN подключении.



## ПРОВЕРКА СВЯЗИ С IT

Убедитесь, что вы точно знаете, как и по какому каналу можно быстро связаться с IT-специалистами при возникновении проблем.



## ПАРОЛЬ ДЛЯ РОУТЕРА

Обязательно смените стандартный пароль домашнего роутера, иначе злоумышленники легко смогут получить доступ к вашим данным.



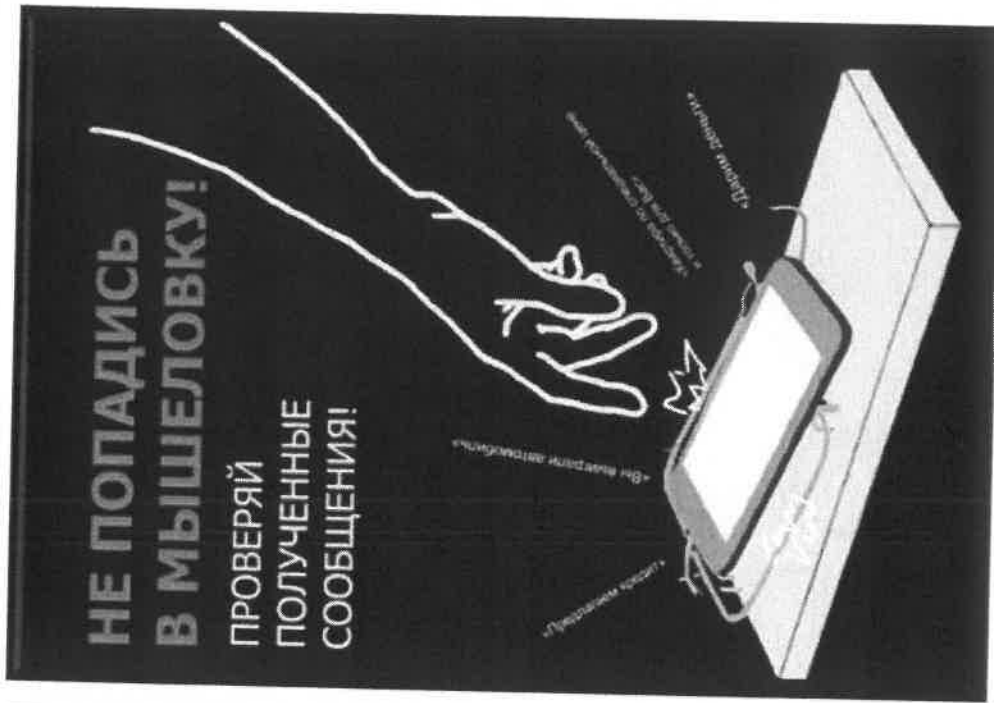
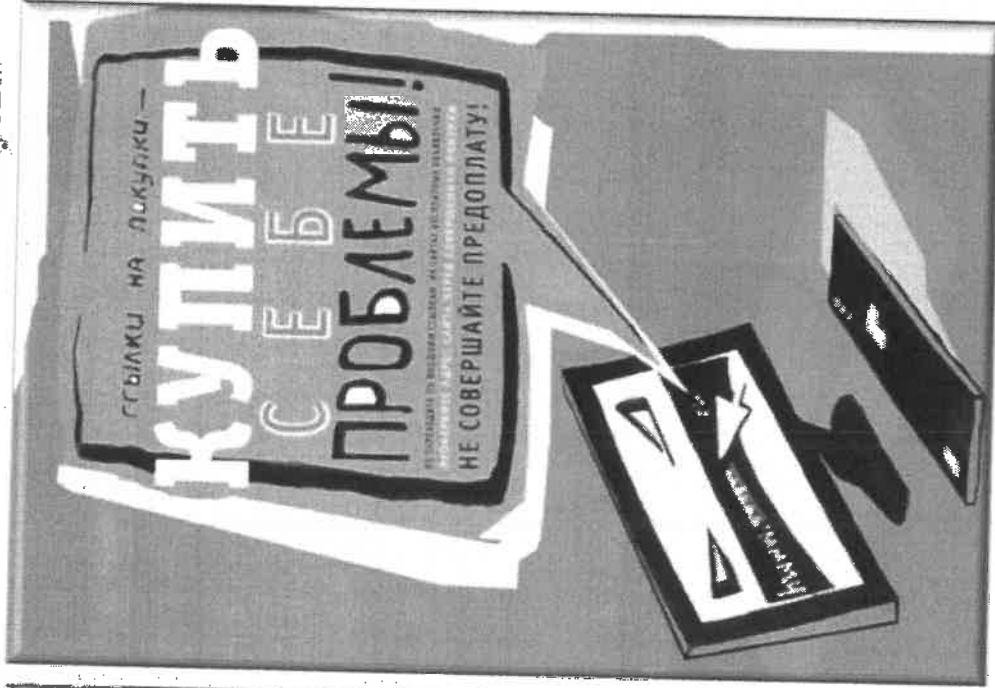
## ДРУГИЕ ПОЛЬЗОВАТЕЛИ

Объясните близким, что вашим рабочим компьютером пользоваться нельзя, чтобы избежать случайного заражения устройства или потери данных.



grouper-ib

Работы победителей регионального конкурса плакатов в рамках профилактической акции  
 «Не дай себя обмануть!»\*



\*Проведён по инициативе общественного совета при УМВД России по Владимирской области.

## Типовой сценарий проведения с детьми учебного занятия на тему «Основные правила безопасности в сети Интернет»



Интернет — уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учёбы. Здесь можно общаться в режиме онлайн, найти новых друзей, вступить в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, — всё это Интернет. Почему мы вынуждены предупреждать об опасностях виртуального мира, если в нём так много всего хорошего и полезного? Достаточно большая часть интернет-пользователей ищет не друзей в Интернете, а свои жертвы. Обезопасить себя не так уж и трудно — достаточно серьёзно отнестись к проблеме кибербезопасности и соблюдать простые правила.

В ходе урока «Безопасный Интернет — детям» мы расскажем об основных направлениях по обеспечению кибербезопасности: как важно уделять внимание парольной политике, кто может интересоваться вашей страницей ВКонтакте, почему не стоит кормить троллей и чем они, в принципе, «питаются».

### Правила для младших школьников:

#### 1. ПАРОЛЬ («ключ от дома»)

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом. Правило первое: «Ключ от дома должен быть секретным, надёжным и только вашим».

#### 2. ВИРУСЫ и АНТИВИРУСЫ («моем руки с мылом»)

Любому гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета. Надо использовать лицензионное антивирусное программное обеспечение. Не скачивайте программные продукты из сомнительных источников. Не отвечайте на непонятные вам рассылки. И главное — не посещайте ресурсы с сомнительной репутацией. Сомневайтесь — не нажимайте «да» или «ENTER».

Держимся подальше от вирусов: «Моем руки с мылом, к вирусам не прикасаемся».

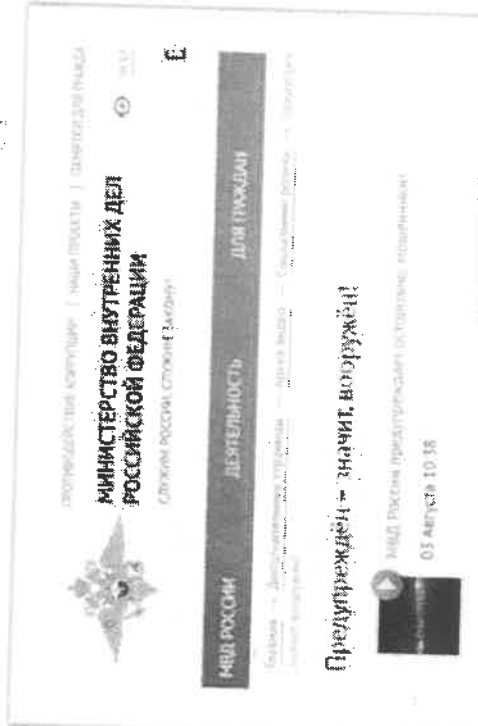
#### 3. ПЕРСОНАЛИЗАЦИЯ («документы — в сейф»)

Никому не давайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы» могут навредить вам. Игнорируйте в сети Интернет подобные запросы. Мы храним свои документы в сейфе, закрываем на ключ, так надо и в Сети охранять свои персональные данные. Третье правило: «Наши документы всегда в сейфе».



# Тематические разделы официального интернет-сайта МВД России

Новостная рубрика  
«Борьба  
с киберпреступностью»



**СНИМАНИЕ НОШЕЧКИ:**

**ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ**

**ПРЕДУПРЕЖДЕН – ЗНАЧИТ, ВОЗВРАЩЕН**

**СОБЕРЕЖЕНИЕ ПОКУПОК В СЕТИ ИНТЕРНЕТ**

**МОШЕННИЧЕСТВА С ПЛАТЕЖНЫМИ КАРТАМИ**

**ВИКНАШ В ЛОТЕРЕЮ**

**МОШЕННИЧЕСТВО ПОД ПРЕДЛОГОМ ДОЛГОВИТЕЛЬНОСТИ**

**МОШЕННОЕ МОШЕННИЧЕСТВО**

**МОШЕННИЧЕСТВА, НАСЛАНЯЕМЫЕ НА ЗАКЛУЧЕНИЕ УСТРОЙСТВА ПОЛЬЗОВАТЕЛЯ ВНЕДОХОДНОЙ ПРОГРАММОЙ**



## Предупрежден – значит, возвращен!

- МВД России предупреждает о краже кошелек 03 августа 10:38
- МВД России предупреждает о краже 21 июля 10:50
- МВД России предупреждает о краже 08 июля 10:50
- МВД России предупреждает о краже 24 апреля 11:50

**МОШЕННИЧЕСТВА С ПЛАТЕЖНЫМИ КАРТАМИ**

Банковские карты – это инструмент для совершения платежей и доступа к различным средствам на счете, не требующий для этого присутствия в банке. Но при этом использование банковской карт оставляет множество лазеек для мошенников.

**ФОРМА ЗАБЛЮДЕНИЯ ПЛАТЕЛЬНОЙ КАРТЫ (ПОТЕРЯЕТЕСЬ В БАНК ЛЮБИТЕ ПЛАТЕЖИ (ПОТЕРЯЕТЕСЬ) ОБ ОТЪЕЗДЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И ОТКЛЮЧЕНИЯ СИСТЕМЫ МОБИЛЬНЫЙ БАНК**

**ФОРМА СТРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Чтобы не стать жертвой злоумышленников при незаконной банковской карте, необходимо придерживаться следующих правил:

Пришло СМС от банка о блокировке карты или аресте ее баланса и сразу сообщите номер карты, пароль и код доступа. Что делать?

Формы и подписание ("зеркальные") сайты

Что такое "банковские" (или мошеннические) сайты?



**МОЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ**

**ИНТЕРПОЛ ПРЕДУПРЕЖДАЕТ АККАУНТ СОЦИАЛЬНОЙ СЕТИ НАРУШАЕТСЯ В ПОСТОЯННОЙ ЗАЩИТЕ!**

**УПРАВЛЕНИЕ «К» ПРЕДУПРЕЖДАЕТ ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ**