

Актуальные способы совершения киберпреступлений

Электронные сервисы, интернет-банкинг, удаленная работа и учеба, социальные сети, интернет-магазины и маркетплейсы – все это настолько прочно вошло в нашу повседневность, что иногда трудно поверить, как жили без этого раньше. Чем больше мы погружаемся в мир информационно-коммуникационных технологий, тем уязвимее становимся для интернет-преступников.

Киберпреступность не стоит на месте, а активно идет в ногу со временем, с развитием технологий меняются схемы и способы обмана. Отдельное беспокойство вызывает применение искусственного интеллекта в преступной деятельности. По статистике женщины (65%) чаще всего становятся жертвами телефонных мошенников, которые выманивают деньги путем психологических манипуляций (77,9%), купли-продажи товаров и оказания услуг (65,6%), благотворительности (100%). Мужчины (84,8%), как правило, становятся жертвами мошенничества, связанного с использованием сайтов знакомств. Большинство потерпевших от интернет-мошенничеств в возрасте от 30 до 49 лет, люди старше 50 лет более подвержены мошенничествам, связанным с помощью родственникам.

Наиболее распространенным способом интернет-хищения денежных средств является **телефонное мошенничество** в различных модификациях.

Телефонные мошенники

ПРЕДСТАВЛЯЮТСЯ:

- сотрудниками гос. органов и банков
- продавцами, инвесторами, брокерами
- работниками служб связи (Белпочта, Белтелеком, А1, МТС)
- работниками коммунальных служб (энергонадзора, водоканала, газовой службы)

УГРОЖАЮТ И ЗАПУГИВАЮТ:

- подозрением в преступлении и проведением обыска
- сложной ситуацией с родственником
- окончанием действия прибора учета или услуги

УБЕЖДАЮТ И ЗАСТАВЛЯЮТ:

- под предлогом декларирования перевести деньги на “безопасный” счет
- внести предоплату за товар или взнос в инвестиционный проект
- передать личные данные и коды из сообщения, установить приложение

Не дайте себя обмануть!

Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

Аферисты представляются работниками банков, коммунальных служб, водоканала, энергонадзора, служб газа и связи, сотрудниками правоохранительных и государственных органов, даже вашими знакомыми и родственниками. Чтобы похитить деньги мошенники под различными предложениями пытаются завладеть личными данными, включая коды из смс. Часто они действуют в паре. Например, первый под предлогом замены ключей от домофона выманивает числовой код из смс, а второй мошенник, представляясь правоохранителем, угрожает проведением обыска и изъятием денежных средств за передачу того самого кода.

Или другой пример. Один мошенник представляется руководителем вашей организации и пугает подозрением в экстремистской деятельности и проведением обыска, а другой от имени правоохранителя предлагает якобы помощь в решении данной проблемы: для этого нужно перевести деньги на «временный счет» или передать их курьеру.

Надо помнить, что никаких временных счетов не бывает и вернуть свои деньги с чужого счета невозможно.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:

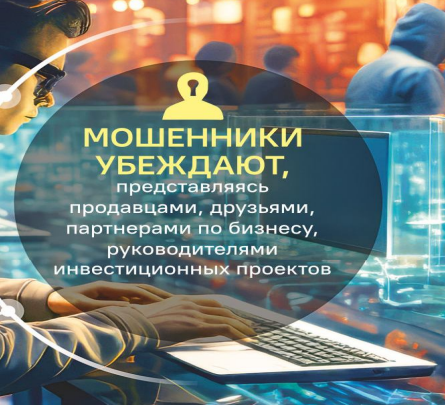


МОШЕННИКИ УБЕЖДАЮТ, представляясь сотрудниками правоохранительных органов, банковских организаций или руководителем вашей организации.

- Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет
- Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет
- Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске
- Передать личные данные и код из смс, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:



МОШЕННИКИ УБЕЖДАЮТ, представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов

- Перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка
- Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)
- Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку
- На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода



Больше информации на сайте <https://mvd.gov.by>



Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

Зарегистрированы случаи, когда подростков под угрозой привлечения к ответственности мошенники заставляли открыть сейф и передать лично курьеру деньги родителей.

Оба следующих случая произошли в октябре этого года в Минском районе.

Школьник после общения с незнакомкой в мессенджере вынес из дома 70 тысяч долларов. В данном случае собеседница узнала геолокацию его школы по отправленному фото, после чего школьник получил видео, в котором человек в балаклаве с украинским флагом сообщил ему, что взломал аккаунт его онлайн-подруги и теперь владеет всей информацией из их переписки. Сразу на связь с парнем вышел неизвестный, который представился сотрудником милиции и сообщил, что передача геолокации иностранцу влечет уголовную ответственность. Вскоре появился еще один псевдомилиционер, который под предлогом декларирования потребовал показать сколько денег имеется в доме. В течение недели мошенники вымогали у парня информацию и угрожали ему. В результате парень узнал у отца код от сейфа и сфотографировал деньги. На следующий день с ним связался якобы сотрудник КГБ, который потребовал срочно передать деньги курьеру. Мальчик положил все деньги в рюкзак и оставил его в лесу. Все действия он транслировал в прямом эфире. Деньги родители собирали на ремонт дома. Во втором случае 15-летнюю девушку неизвестный по телефону убедил, что необходимо задекларировать все сбережения родителей. По его указанию она отдала курьеру 55 тысяч долларов. Деньги родители копили ей на квартиру.

Также мошенники используют и другие схемы обмана. Аферист по телефону представляется работником банка или предприятия связи (Белтелеком, А1, МТС) и убеждает обновить мобильное приложение, для чего необходимо скачать и установить на телефон поддельное приложение, направленное ссылкой или файлом (*.apk) в мессенджере.

Часто такие фейковые приложения предоставляют удаленный доступ к устройству и мошенник «подсматривает» все, что происходит на экране. Иногда этого бывает достаточно, чтобы похитить деньги. В последнее время появилась еще одна возможность. После установки приложения мошенник просит передать пин-код и поднести банковскую карту к задней крышке телефона (к модулю NFC). Так мошенник получает дубликат вашей банковской карты и тоже может похитить деньги.

Нельзя выполнять никаких действий, связанных с финансами, по указанию незнакомых, кем бы они не представились.

Больше всего людей становятся жертвами киберпреступников при попытке купить товар подешевле в социальных сетях или мессенджерах. Часто в мошеннических аккаунтах «продают» одежду, смартфоны, автомобильные шины, садовые кресла, цветы, рыбу и многое другое, то, что нужно доставлять курьером, а не почтой.

Остерегайтесь подозрительно низких цен и не переводите предоплату за товар или услугу, выбирайте оплату наложенным платежом. Прежде чем согласиться на покупку, проверьте наличие у продавца сайта в белорусском сегменте интернета и созвонитесь с ним по телефону. Тщательно проверяйте информацию о продавце.

Наряду с указанными крупные хищения мошенники совершают с использованием поддельных инвестиционных или криптоплатформ. Размещая рекламу в Интернете, они могут использовать видео с известными людьми – политиками, спортсменами, даже блогерами, которые озвучены фразами, сгенерированными с помощью искусственного интеллекта. Например, на видео может быть известная телеведущая, которая в репортаже рассказывает о якобы новой возможности заработка, или заместитель министра дает интервью, что многие уже пользуются определенным ресурсом и получают деньги, хотя на самом деле все слова – это всего лишь результат работы нейросетей. С заинтересовавшимися связываются так называемые кураторы или брокеры и убеждают участвовать в инвестировании или программе на том самом ресурсе. Для получения пассивного дохода предлагают вложить деньги в прибыльный проект. Часто жертв побуждают к оформлению кредитов для перевода большей суммы. На самом деле вкладчику просто «рисуют» его прибыль на сайте и никогда не дают возможности вывести его деньги.

Нужно понимать, что легких денег не бывает, а бесплатный сыр в мышеловке. Вернуть деньги, «вложенные» подобным образом, невозможно.

Одним из новых, набирающих обороты, способов является вымогательство за разблокировку Iphone. Вначале аферист в переписке узнает о наличии Iphone у будущей жертвы, а потом под различными предлогами убеждает войти в его iCloud. Предлогами могут быть, например, помощь в восстановлении фотографий, сохранение диплома, возможность пройти уровень в игре или получить для своего героя игровое имущество, оружие или способность. После входа в iCloud мошенника, Iphone жертвы блокируется. Для его разблокировки предлагается заплатить сумму, в зависимости от модели, превышающую 1000 рублей.

Это не все, но самые актуальные и распространенные схемы, и со временем они могут меняться. Чтобы не стать жертвой киберпреступников, необходимо всегда адекватно оценивать свои действия и как бы вас не запугивали, не поддаваться панике и страху. Будьте бдительны и берегите свои деньги!

Главное управление
по противодействию киберпреступности
криминальной милиции
МВД Республики Беларусь

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с **неизвестного**
номера

2 

звонящий
представляется
вашим
родственником

3 

он говорит,
что **сбил человека**
или из-за него
человек
попал в ДТП

4 

он просит **денег**,
как **компенсацию**
вреда или
чтобы **(замыть) дело**

5 

затем звонит
«милиционер»/
«следователь»
и подтверждает
легенду

6 

за деньгами
приезжает
курьер

Мама, папа, я
в беде!

Нужны деньги!
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102

! ВНИМАНИЕ, ОПАСНОСТЬ !

ЗАЩИТИТЕ СЕБЯ ОТ МОШЕННИКОВ:

НЕ ПЕРЕХОДИТЕ по ссылкам и письмам от
незнакомцев, не нажимайте на картинки и кнопки...

НЕ ВЕРЬТЕ обещаниям внезапных выигрышей

НЕ ИСПОЛЬЗУЙТЕ одинаковые пароли для всех
аккаунтов

НЕ УКАЗЫВАЙТЕ личную информацию в открытых
источниках

НЕ СООБЩАЙТЕ свои персональные данные
и данные банковской карты



НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

**Если вы или ваши близкие стали
жертвами мошенников, или вы
подозреваете, что в отношении вас
планируются противоправные действия
НЕЗАМЕДЛИТЕЛЬНО СООБЩАЙТЕ В МИЛИЦИЮ!**

102



mvd.gov.by



© 2015 Республиканское государственное учреждение «Министерство внутренних дел Республики Беларусь»

Безопасный интернет для детей

**СОХРАНИ
ИНФОРМАЦИЮ**

**не сообщай незнакомцам
свой логин и пароль**

**не открывай файлы из
непроверенных источников**

**не заходи на сайты, которые
защита компьютера считает
подозрительными**



**НЕ отправляй незнакомцам
свои фото и видео**

Злоумышленники могут узнать что-то
нужное им о твоей жизни

**ГЛАВНЫЕ
ПРАВИЛА
ЦИФРОВОЙ
ГИГИЕНЫ**



**НЕ встречайся с людьми,
с которыми знаком только
в интернете**

За маской онлайн-собеседника
может скрываться злоумышленник



**НЕ сообщай в интернете
свой реальный
адрес и телефон**

Злоумышленник может встретить
тебя с недобрыми намерениями



**НЕ отправляй личные данные
для участия в конкурсах
на малоизвестных сайтах**

Информацией могут завладеть и
воспользоваться недоброжелатели

**РОДИТЕЛИ!
научите детей
пользоваться
интернетом
правильно!**



**Всегда важно помнить: неправильное поведение
в интернете может принести большой вред.**



не дай себя обмануть!



**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ**

**круглосуточный
единый
номер**

102

Как не превратить iPhone в «кирпич»

Мошенники используют различные уловки, чтобы заблокировать ваше устройство, вынуждая войти в их учётную запись Apple (iCloud)

Основные схемы обмана

- ✗ **«Помощь с файлами»**
Ссылаясь на «неисправное устройство», просят помощи в доступе к файлам (фотографиям, документам и т.д.) из облачного хранилища iCloud путем авторизации в мошеннической учётной записи
- ✗ **«Бесплатные игры и приложения»**
Рекламируют доступ к играм («PUBG Mobile», «Standoff 2») и приложениям («AioGram») в TikTok или Telegram, предлагая установить их через предоставленный аккаунт Apple
- ✗ **«Работа/подработка»**
Обещают вакансию (часто связанную с тестированием приложений), но требуют входа в «корпоративный» аккаунт Apple

Как защитить себя

- ✓ не сообщайте никому свои учётные данные (логин и пароль) от аккаунта Apple (iCloud)
- ✓ не входите на своём мобильном устройстве в аккаунт Apple (iCloud), предоставленный незнакомцами из Интернета
- ✓ не переходите по неизвестным ссылкам и не вводите данные Apple ID на посторонних сайтах

ВАЖНО!

Если ваш аккаунт заблокирован мошенником, сервисные центры не помогут. Разблокировка возможна только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

БОЛЬШЕ ИНФОРМАЦИИ

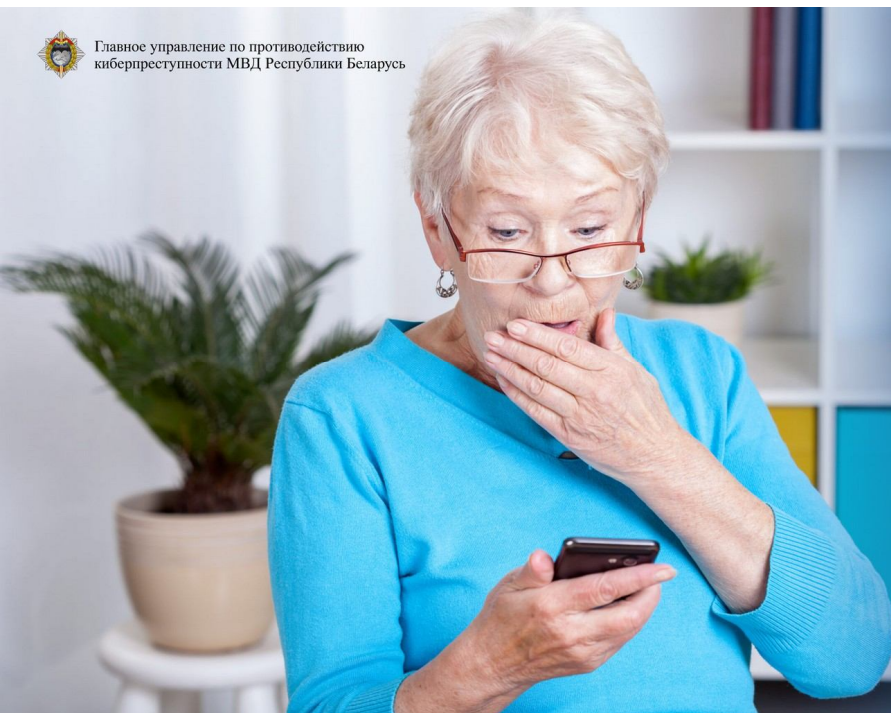
В Telegram-канале
КИБЕРКРЕПОСТЬ
[CYBER_FORTRESS_BREST](#)



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



НАУЧИТЕ

РОДИТЕЛЕЙ

**ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ**