МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ПАМЯТКА

«Об основных мошеннических схемах в сфере информационных технологий в отношении граждан и способах защиты от них»

Минск 2026

Разработчики:

В.Ю.Мезяк, старший преподаватель кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь», подполковник милиции

Распознавание и предотвращение мошеннических схем с подменой QR-кодов

Мошенники массово подменяют настоящие QR-коды для оплаты в общественных местах. Аферисты изготавливают фейковые стикеры с QR-кодами, которые визуально очень похожи на оригинальные, и наклеивают их поверх или рядом с настоящими кодами.

Где чаще всего происходит подмена:

Вокзалы и аэропорты (стойки информации, автоматы по продаже билетов, вендинговые аппараты, парковки);

Кафе и рестораны (наклеивают вечером поверх QR-меню на столиках);

Общественный транспорт, остановки, метро;

Парковки и автозаправки;

Торговые центры и магазины (коды для оплаты товаров, услуг, бонусных карт).

Пользователь сканирует QR-код камерой смартфона, чтобы быстро оплатить услугу или заказ. Вместо перехода на официальную страницу оплаты он попадает на поддельный фишинговый сайт, который полностью имитирует интерфейс банка, сервиса оплаты или официального приложения.

На сайте отображается сумма платежа, название услуги и форма для ввода реквизитов банковской карты (номер карты, срок действия, CVV/CVC, имя держателя). После ввода данных они мгновенно передаются злоумышленникам. В дальнейшем полученная информация может использоваться для кражи денег, оформления микрозаймов, совершения других покупок или продажи в даркнете.

Схема активно использует элементы социальной инженерии: удобство и скорость оплаты, доверие к привычному способу платежа и отсутствие видимых признаков опасности на первый взгляд.

Ключевые советы, чтобы не попасть в такую ситуацию:

Внимательно осматривайте QR-код перед сканированием.

Если стикер выглядит новым, неровно наклеенным, имеет следы клея, отличается по цвету, качеству печати или расположен поверх оригинального – не сканируйте его.

Не используйте QR-коды для оплаты в общественных местах.

Предпочитайте оплату через официальное мобильное приложение банка или сервиса, вводя реквизиты вручную или через NFC. При сомнениях выбирайте наличный расчёт или другой проверенный способ.

Рекомендация:

При любом подозрении на подмену QR-кода лучше перестраховаться и отказаться от сканирования. Регулярно напоминайте себе: «Лучше потратить чуть больше времени, чем потерять деньги». Это один из самых распространённых и эффективных методов мошенничества с бесконтактными платежами в настоящее время.

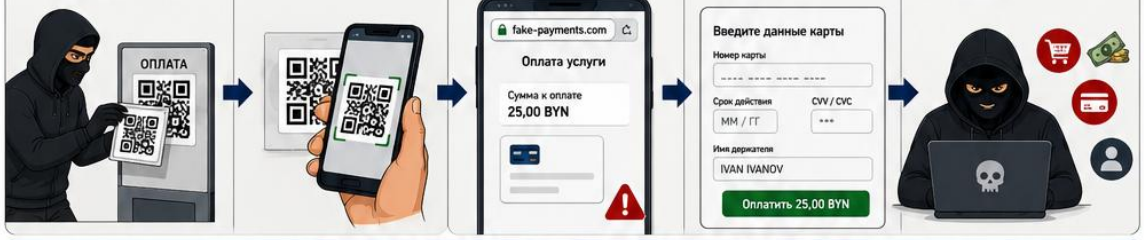
ОСТОРОЖНО! МОШЕННИКИ ПОДМЕНЯЮТ QR-КОДЫ ДЛЯ ОПЛАТЫ

Республика Беларусь

Сканируя поддельный QR-код, вы рискуете потерять деньги и передать данные своей карты мошенникам!

КАК РАБОТАЕТ СХЕМА

1. Мошенники изготавливают стикеры с поддельными QR-кодами и наклеивают их поверх или рядом с настоящими кодами.
2. Вы сканируете QR-код камерой смартфона, чтобы быстро оплатить услугу или заказ.
3. Вместо официальной страницы оплаты вы попадаете на фишинговый сайт-подделку.
4. Вы вводите данные карты на поддельном сайте. Данные мгновенно передаются мошенникам.
5. Мошенники используют ваши данные для кражи денег, оформления займов, покупок или продажи в даркнете.



ГДЕ ЧАЩЕ ВСЕГО ПРОИСХОДИТ ПОДМЕНА QR-КОДОВ

Вокзалы и аэропорты
стойки информации, билеты, вендинговые аппараты, парковки

Кафе и рестораны
наклеивают вечером поверх QR-меню на столиках

Общественный транспорт, остановки, метро

Парковки и автозаправки

Торговые центры и магазины
коды для оплаты товаров, услуг, бонусных карт



КАК ОТЛИЧИТЬ ПОДДЕЛКУ?

Настоящий QR-код

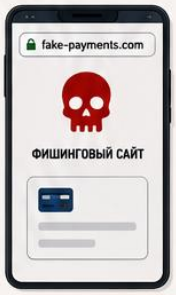
- Ровно наклеен
- Чистый, без следов клея
- Цвет и качество печати соответствуют оригиналу
- Нет дополнительных наклеек сверху

Поддельный QR-код

- Неровно наклеен
- Имеет следы клея, пузыри, загнутые края
- Отличается цветом, качеством печати
- Наклеен поверх оригинального кода

ЧЕМ ОПАСЕН ПОДДЕЛЬНЫЙ QR-КОД?

- Кража денег с вашей карты
- Оформление кредитов и микрозаймов на ваше имя
- Совершение покупок и переводов от вашего имени
- Продажа ваших данных в даркнете



КАК НЕ ПОПАСТЬ НА УЛОВКУ МОШЕННИКОВ?

1. ВНИМАТЕЛЬНО ОСМАТРИВАЙТЕ QR-КОД
Проверяйте, как наклеен стикер, его состояние, цвет и качество печати. При малейших сомнениях – не сканируйте.

2. НЕ ИСПОЛЬЗУЙТЕ QR-КОДЫ ДЛЯ ОПЛАТЫ В ОБЩЕСТВЕННЫХ МЕСТАХ
Это повышает риск попасть на поддельный сайт и потерять деньги.

3. ПРЕДПОЧИТАЙТЕ ОПЛАТУ ЧЕРЕЗ ОФИЦИАЛЬНОЕ ПРИЛОЖЕНИЕ БАНКА ИЛИ СЕРВИСА
Вводите реквизиты вручную или используйте NFC. Это безопаснее.

4. ПРИ СОМНЕНИЯХ – ВЫБИРАЙТЕ ДРУГОЙ СПОСОБ ОПЛАТЫ
Оплатите наличными или воспользуйтесь проверенным способом.

РЕКОМЕНДАЦИЯ:

При любом подозрении на подмену QR-кода лучше перестраховаться и отказаться от сканирования. Регулярно напоминайте себе: «Лучше потратить чуть больше времени, чем потерять деньги». Это один из самых распространённых и эффективных методов мошенничества с бесконтактными платежами в настоящее время.



ЗАПОМНИТЕ ГЛАВНОЕ:

- ✓ Не торопитесь
- ✓ Проверяйте QR-код
- ✓ Используйте безопасные способы оплаты
- ✓ Берегите свои деньги и данные!

БУДЬТЕ БДИТЕЛЬНЫ! ВАША ВНИМАТЕЛЬНОСТЬ – ЛУЧШАЯ ЗАЩИТА ОТ МОШЕННИКОВ!

Распознавание и предотвращение мошеннических схем с «поддельными штрафами на дачах»

Мошенники массово рассылают владельцам дач и загородных участков фальшивые уведомления о якобы выявленных нарушениях. Сообщения приходят по SMS или электронной почте и выглядят максимально официально: содержат номер постановления, сумму штрафа, дату нарушения, а часто и предложение оплатить со скидкой (например, 50%).

Темы нарушений типичные для дачных участков: спил деревьев без разрешения, незаконные постройки, нарушение правил землепользования, пожарной безопасности и т.д. Расчёт делается на страх и спешку владельцев – человек быстро переводит деньги, не проверяя информацию.

После перехода по ссылке или при оплате через предложенные реквизиты/QR-код данные банковской карты или доступ к счету попадают к злоумышленникам. Схема активно использует социальную инженерию: официальный стиль документа, ощущение срочности и апелляцию к реальным нормам законодательства.

Ключевые советы, чтобы не попасть в такую ситуацию:

Никогда не оплачивайте штрафы по ссылкам или реквизитам из писем/сообщений.

Любое постановление проверяйте только через официальные государственные сервисы (Единый портал электронных услуг e.gov.by, личный кабинет на сайте исполкома или ГАИ/Минприроды).

Не реагируйте на сообщения с требованием срочной оплаты.

Государственные органы не присылают штрафы на дачные участки по SMS или e-mail с прямым требованием перевести деньги. Официальные уведомления приходят заказным письмом или через личный кабинет.

Рекомендация:

При получении любого подозрительного уведомления о штрафе на даче – остановитесь и проверьте информацию исключительно официальным способом. Если сомневаетесь – обратитесь в соответствующие компетентные органы.

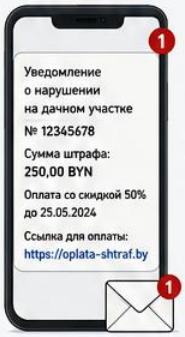
ОСТОРОЖНО! МОШЕННИКИ РАССЫЛАЮТ «ПОДДЕЛЬНЫЕ ШТРАФЫ НА ДАЧАХ»

Республика Беларусь

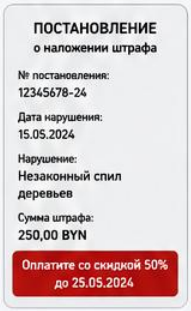
Мошенники пугают владельцев дач и загородных участков фальшивыми штрафами и выманивают деньги.

КАК РАБОТАЕТ СХЕМА

1. Вы получаете SMS или e-mail с уведомлением о штрафе.



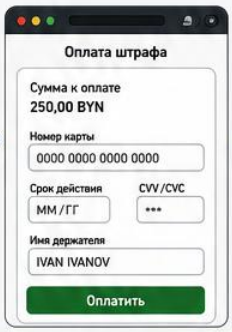
2. Сообщение выглядит официально: номер постановления, дата нарушения, сумма, скидка.



3. Вы переходите по ссылке или сканируете QR-код для оплаты.



4. Попадаете на поддельный сайт, вводите данные банковской карты или счета.



5. Деньги списываются, а ваши данные попадают к мошенникам.



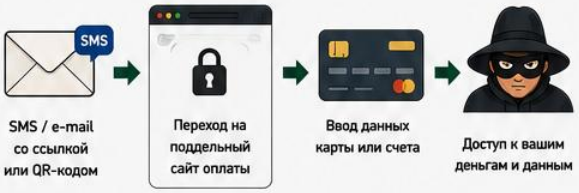
НА КАКИЕ «НАРУШЕНИЯ» ССЫЛАЮТСЯ МОШЕННИКИ

- Спил деревьев без разрешения
- Незаконные постройки
- Нарушение правил землепользования
- Нарушение правил пожарной безопасности
- И другие «нарушения» на дачных участках



Расчёт на страх и спешку!
Вы быстро переводите деньги, не проверяя информацию.

КАК МОШЕННИКИ ПОЛУЧАЮТ ВАШИ ДАННЫЕ И ДЕНЬГИ



SMS / e-mail со ссылкой или QR-кодом → Переход на поддельный сайт оплаты → Ввод данных карты или счета → Доступ к вашим деньгам и данным

Полученные данные могут использоваться для кражи денег, оформления микрозаймов, покупок и продажи в даркнете.

КАК НЕ ПОПАСТЬСЯ НА УЛОВКУ МОШЕННИКОВ?

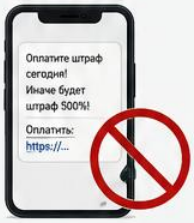
1. **НИКОГДА НЕ ОПЛАЧИВАЙТЕ ШТРАФЫ ПО ССЫЛКАМ ИЛИ РЕКВИЗИТАМ ИЗ ПИСЕМ/СООБЩЕНИЙ.**



2. **ПРОВЕРЯЙТЕ ЛЮБОЕ ПОСТАНОВЛЕНИЕ ТОЛЬКО ЧЕРЕЗ ОФИЦИАЛЬНЫЕ ГОСУДАРСТВЕННЫЕ СЕРВИСЫ.**

e.gov.by (единый портал электронных услуг) | Личный кабинет на сайте исполкома | Сайты ГАИ, Минприроды и др.

3. **НЕ РЕАГИРУЙТЕ НА СООБЩЕНИЯ С ТРЕБОВАНИЕМ СРОЧНОЙ ОПЛАТЫ.**



4. **ГОСУДАРСТВЕННЫЕ ОРГАНЫ НЕ ПРИСЫЛАЮТ ШТРАФЫ НА ДАЧНЫЕ УЧАСТКИ ПО SMS ИЛИ E-MAIL С ТРЕБОВАНИЕМ ПЕРЕВЕСТИ ДЕНЬГИ.**



Официальные уведомления приходят заказным письмом или через личный кабинет.

РЕКОМЕНДАЦИЯ

- При получении подозрительного уведомления о штрафе на даче — остановитесь и проверьте информацию исключительно официальным способом.
- Используйте только официальные сайты и сервисы. Не переходите по ссылкам из сомнительных сообщений.
- Если сомневаетесь – обратитесь в соответствующие компетентные органы.

КАК ПРОВЕРИТЬ ИНФОРМАЦИЮ О ШТРАФЕ?

1. Зайдите на e.gov.by или сайт вашего исполкома.
2. Войдите в личный кабинет.
3. Проверьте наличие постановлений и штрафов.
4. При необходимости свяжитесь с органом напрямую по официальным контактам.



ПОМНИТЕ! ЛУЧШЕ ПОТРАТИТЬ ЧУТЬ БОЛЬШЕ ВРЕМЕНИ, ЧЕМ ПОТЕРЯТЬ ДЕНЬГИ!

БУДЬТЕ БДИТЕЛЬНЫ! ЗАЩИТИТЕ СЕБЯ И СВОИ ДЕНЬГИ!

Распознавание и предотвращение мошеннических схем с кражей Telegram-аккаунтов

Мошенники рассылают пользователям сообщения якобы от администрации Telegram с предупреждением о скором удалении учётной записи. В сообщении содержится требование срочно «отменить процедуру удаления» по ссылке или кнопке.

Как только жертва переходит по ссылке и вводит полученный код авторизации (SMS или из приложения), мошенники мгновенно получают полный доступ к аккаунту. Далее аккаунт может использоваться для рассылки спама, мошенничества контактам жертвы, кражи данных или продажи.

Схема активно эксплуатирует страх потери аккаунта и доверие к бренду Telegram.

Ключевые советы, чтобы не попасть в такую ситуацию:

Никогда не переходите по ссылкам из подозрительных сообщений и не вводите коды авторизации. Официальная администрация Telegram **никогда** не просит коды подтверждения через ссылки или сообщения.

Проверяйте источник сообщения. Официальные сервисные аккаунты Telegram не имеют статуса «был(а) недавно», не предлагают добавить в контакты или заблокировать. Обращайте внимание на дату создания аккаунта и страну – у настоящих служб они давно зарегистрированы.

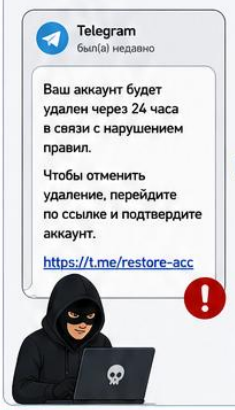
Рекомендация: При получении любого уведомления об удалении аккаунта или других критических действиях в Telegram – игнорируйте сообщения и проверьте информацию только внутри официального приложения. Никому и никогда не передавайте коды подтверждения.

ОСТОРОЖНО! МОШЕННИКИ КРАДУТ TELEGRAM-АККАУНТЫ!

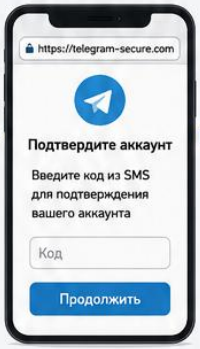
Мошенники рассылают сообщения якобы от администрации Telegram с предупреждением о скором удалении аккаунта. Их цель – получить ваш код авторизации и завладеть вашим аккаунтом.

КАК РАБОТАЕТ СХЕМА

1 Вы получаете сообщение якобы от администрации Telegram.



2 Вы переходите по ссылке и попадаете на поддельный сайт, который выглядит как настоящий.



3 Вам приходит код авторизации (SMS или из приложения).



4 Вы вводите код на поддельном сайте.



12345

Мошенники получают доступ к вашему аккаунту.

5 Ваш аккаунт используется для рассылки спама, мошенничества, кражи данных или продажи.

- Рассылка спама
- Обман ваших контактов
- Кража данных
- Продажа аккаунта в интернете

ПРИЗНАКИ ОБМАНА

- Сообщение о «скором удалении аккаунта» или других угрозах.
- Ссылка ведёт на сторонний сайт, не связанный с официальным доменом Telegram.
- Требуют срочно ввести код из SMS или приложения.
- Отправитель просит добавить его в контакты или предлагает «помощь».
- У аккаунта отправителя статус «был(а) недавно», короткая история или недавняя дата создания.



КАК ПРОВЕРИТЬ ИСТОЧНИК СООБЩЕНИЯ

ОФИЦИАЛЬНЫЙ АККАУНТ

Telegram ✓
служебные уведомления
был(а) очень давно

- Имеет значок подтверждения (галочка).
- Не имеет статуса «был(а) недавно».
- Не пишет первым и не требует никаких данных.
- Дата создания: давно.
- Официальная страна: обычно ОАЭ.

МОШЕННИК

Telegram Support
был(а) недавно

- Нет значка подтверждения.
- Статус «был(а) недавно».
- Может писать первым и требовать коды, данные, добавление в контакты.
- Дата создания: недавно.
- Страна может быть любой.

КАК НЕ ПОПАСТЬСЯ НА УЛОВКУ МОШЕННИКОВ

1. НИКОГДА НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ

Не переходите по ссылкам из сообщений от незнакомых или подозрительных аккаунтов.

2. НЕ ВВОДИТЕ КОДЫ АВТОРИЗАЦИИ



Официальная администрация Telegram никогда не просит коды подтверждения через сообщения или сайты.

3. ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ ТОЛЬКО В ПРИЛОЖЕНИИ

Проверяйте уведомления и статус аккаунта только в официальном приложении Telegram.

4. НЕ ДАВАЙТЕ ДОСТУП К СВОЕМУ АККАУНТУ

Никому и никогда не передавайте коды, данные или доступ к аккаунту.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС УЖЕ ОБМАНУЛИ

- Срочно завершите все активные сессии в Telegram: Настройки → Устройства → Завершить все другие сеансы.
- Измените облачный пароль и включите двухэтапную аутентификацию.
- Сообщите близким и контактам, что ваш аккаунт мог быть взломан.
- Обратитесь в техподдержку Telegram через официальное приложение.

ВАЖНО ЗНАТЬ!

- Telegram не отправляет SMS или сообщения с требованием ввести код для «отмены удаления».
- Удаление аккаунта происходит только из-за бездействия (если вы не заходили в аккаунт длительное время).
- Будьте бдительны! Мошенники используют страх, спешку и доверие к бренду Telegram.



Будьте внимательны! Никому и никогда не передавайте коды подтверждения!
Ваша бдительность – лучшая защита вашего аккаунта!

Распознавание и предотвращение мошеннических схем с фейковыми аккаунтами руководителей военкоматов

С фейкового аккаунта в мессенджере (Telegram, Viber, WhatsApp и др.), который выдаёт себя за руководителя одного из военного комиссариата, приходит сообщение. Мошенник пишет о якобы возникшей внештатной ситуации, проблемах с документами, призыве, отсрочке или других служебных вопросах, напрямую касающихся получателя или его близких.

Создаётся сильное ощущение срочности и психологического давления: «вопрос нужно решить сегодня», «иначе будут последствия», «ситуация критическая». После первого контакта мошенник «переключает» жертву на второго участника схемы – якобы специалиста, юриста или сотрудника, который «может помочь решить вопрос».

Далее под различными предлогами выманивают конфиденциальную информацию: паспортные данные, логины и пароли от государственных сервисов, коды из SMS, реквизиты банковских карт, доступ к аккаунтам. В некоторых случаях просят перевести деньги «на решение вопроса» или «для оформления документов».

Цель схемы – использовать доверие к государственным структурам и страх перед военным комиссариатом, чтобы сбить человека с толку и получить данные или деньги.

Ключевые советы, чтобы не попасть в такую ситуацию:

Никогда не поддавайтесь на сообщения от «начальства» в мессенджерах с просьбами о срочной помощи или предоставлении данных. Проверяйте любую информацию только через официальные каналы связи (личный звонок, служебная почта, внутренние системы).

При получении подозрительного сообщения сразу сообщайте реальному руководству. Не отвечайте мошеннику и предупреждайте коллег. Фейковые аккаунты часто используют похожие имена, фото и стиль общения.

Рекомендация: Если приходит подобное сообщение якобы от руководителя военкомата или любого другого начальника – сохраняйте спокойствие, не выполняйте никаких указаний и немедленно докладывайте лично.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ

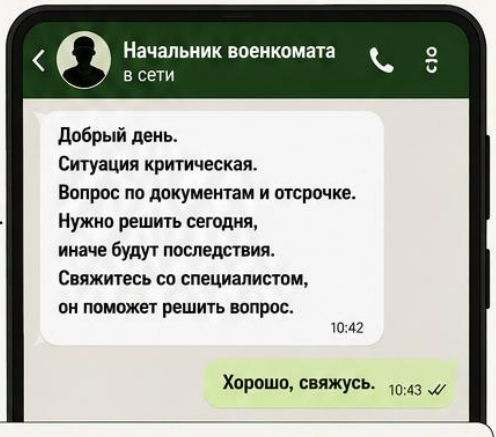
С ФЕЙКОВЫМИ АККАУНТАМИ РУКОВОДИТЕЛЕЙ ВОЕНКОМАТОВ



и др.

С фейкового аккаунта в мессенджере (Telegram, Viber, WhatsApp и др.), который выдаёт себя за руководителя одного из военного комиссариата, приходит сообщение.

Мошенник пишет о якобы возникшей внештатной ситуации, проблемах с документами, призыве, отсрочке или других служебных вопросах, напрямую касающихся получателя или его близких.





Создаётся сильное ощущение срочности и психологического давления:

- «вопрос нужно решить сегодня»
- «иначе будут последствия»
- «ситуация критическая»

После первого контакта мошенник «переключает» жертву на второго участника схемы – якобы специалиста, юриста или сотрудника, который «может помочь решить вопрос».



«Начальник военкомата»

«Специалист», «юрист», «сотрудник»



Далее под различными предлогами выманивают конфиденциальную информацию:

- паспортные данные
- логины и пароли от гос. сервисов
- коды из SMS
- реквизиты банковских карт, доступ к аккаунтам
- перевод денег «на решение вопроса» или «для оформления документов»

Цель схемы – использовать доверие к государственным структурам и страх перед военным комиссариатом, чтобы сбить человека с толку и получить данные или деньги.



КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАСТЬ В ТАКУЮ СИТУАЦИЮ:



Никогда не поддавайтесь на сообщения от «начальства» в мессенджерах с просьбами о срочной помощи или предоставлении данных. Проверяйте любую информацию только через официальные каналы связи (личный звонок, служебная почта, внутренние системы).



При получении подозрительного сообщения сразу сообщайте реальному руководству. Не отвечайте мошеннику и предупреждайте коллег. Фейковые аккаунты часто используют похожие имена, фото и стиль общения.



РЕКОМЕНДАЦИЯ:

Если приходит подобное сообщение якобы от руководителя военкомата или любого другого начальника – сохраняйте спокойствие, не выполняйте никаких указаний и немедленно докладывайте лично.



Распознавание и предотвращение мошеннических схем с «перерасчетом пенсии»

Мошенники обзванивают пенсионеров, представляясь сотрудниками пенсионного фонда, социальной службы или банка. Под предлогом «перерасчета пенсии», «положенных доплат», «индексации» или «оформления новых выплат» они выманивают персональные данные: серию и номер паспорта, дату рождения, номера банковских карт, CVV-коды и другие сведения.

После получения данных в дело вступает второй мошенник, который звонит якобы от имени сотрудника милиции или службы безопасности. Он сообщает, что личные данные пенсионера якобы используются в незаконных финансовых операциях (мошенничестве, отмывании денег и т.д.). Чтобы «защитить» сбережения, пожилого человека убеждают снять все деньги со счетов и передать их «курьеру» (часто тоже мошеннику) для якобы «декларирования», «заморозки» или «безопасного хранения».

Схема построена на высоком доверии пожилых людей к государственным органам, страхе потерять пенсию, чувстве тревоги и сильном психологическом давлении («время ограничено», «иначе всё пропадёт»). В результате пенсионеры теряют крупные суммы.

Ключевые советы, чтобы не попасть в такую ситуацию:

Никогда не сообщайте личные данные (паспорт, карты, коды) по телефону, даже если звонят якобы из пенсионного фонда, банка или милиции. Официальные сотрудники не запрашивают такую информацию по телефону.

При любом звонке с требованием снять деньги или передать их кому-либо – немедленно прекратите разговор. Не передавайте деньги курьерам и не выполняйте указания незнакомцев. Сразу звоните в милицию по номеру 102.

Рекомендация: Предупредите пожилых родственников и коллег: любые звонки о пенсиях, перерасчетах или угрозах по поводу денег – это почти всегда мошенничество. Лучше положить трубку и самостоятельно проверить информацию через официальные контакты организаций.

ОСТОРОЖНО!
МОШЕННИКИ С «ПЕРЕРАСЧЕТОМ ПЕНСИИ»

Республика Беларусь

Не дайте себя обмануть и потерять свои сбережения!

КАК РАБОТАЕТ СХЕМА

1 Первый звонок: «перерасчет пенсии»

Мошенник представляется сотрудником пенсионного фонда, соцслужбы или банка. Под предлогом «перерасчета пенсии», «доплат», «индексации» выманивает личные данные.



- Паспортные данные
- Дата рождения
- Номер карты
- CVV-код и др.

2 Второй звонок: «из милиции»

Звонит другой мошенник, представляется сотрудником милиции или службы безопасности. Сообщает, что ваши данные якобы используются в незаконных операциях.



3 Передача денег курьеру

Пенсионера убеждают снять все деньги и передать их «курьеру» (часто тоже мошеннику).



ЧЕМ ЭТО ОПАСНО?

- Потеря всех сбережений
- Кража личных данных и доступ к счетам
- Использование ваших данных в противоправных целях
- Сильный стресс и психологическое давление на пожилых людей

КАК НЕ ПОПАСТЬ В ТАКУЮ СИТУАЦИЮ?

1 Никогда не сообщайте личные данные по телефону

Официальные сотрудники пенсионного фонда, банка или милиции не запрашивают по телефону:



- паспортные данные
- реквизиты банковских карт
- CVV-коды и пароли
- коды из SMS и приложений



2 Не выполняйте указания незнакомцев

Если вам звонят с требованием снять деньги или передать их кому-либо:

- немедленно прекратите разговор
- не передавайте деньги курьерам
- не выполняйте никаких указаний
- сразу звоните в милицию



ВАЖНО ЗНАТЬ!

- Звонки о «перерасчете пенсии», «доплатах» или «индексации» – это почти всегда мошенники.
- Не доверяйте звонкам о подозрительных операциях и угрозам по поводу денег.
- Лучше положить трубку и самостоятельно проверить информацию через официальные контакты организаций.

КУДА ОБРАЩАТЬСЯ?

- **Пенсионный фонд** – только по официальным номерам телефонов и через их сервисы
- **Банки** – только по номерам, указанным на официальных сайтах или на обороте карты
- В случае подозрений на мошенничество – звоните в милицию по номеру – **102**

ПРЕДУПРЕДИТЕ СВОИХ БЛИЗКИХ!

Расскажите пожилым родственникам и соседям об этих схемах обмана.

Ваша забота может уберечь их от потери денег и стресса!



БУДЬТЕ БДИТЕЛЬНЫ – ЗАЩИТИТЕ СЕБЯ И СВОИХ БЛИЗКИХ!

Распознавание и предотвращение мошеннических схем с «обновлением данных в медкарте»

Мошенники активно рассылают сообщения в Telegram, WhatsApp и других мессенджерах от имени поликлиник, больниц и других учреждений здравоохранения. Они просят «уточнить» или «обновить» персональные и медицинские данные для электронной медицинской карты: рост, вес, дату рождения, группу крови, хронические заболевания и другие сведения.

Для усиления давления мошенники используют предлог «медреформы» и пугают серьёзными последствиями: якобы без актуальной электронной карты человека не пустят на работу, в учебные заведения, не оформят ребёнка в сад/школу или не окажут медицинскую помощь.

Далее схема развивается по одному из сценариев:

Пользователю обещают «звонок от робота», который продиктует «номер талона» или код, и просят переслать его в чат.

Или сразу просят ввести код подтверждения из SMS, пришедший на телефон.

В обоих случаях это позволяет злоумышленникам получить доступ к мессенджеру или аккаунту на государственном портале, после чего они могут похитить дополнительные данные, войти в банковские приложения или продолжить мошенничество от имени жертвы.

Схема рассчитана на доверие людей к медицинским учреждениям и страх перед возможными проблемами со здоровьем и документами.

Ключевые советы, чтобы не попадать в такую ситуацию:

Никогда не предоставляйте личные данные и не вводите коды из SMS по запросам из мессенджеров, даже если они приходят якобы от поликлиники или больницы.

Игнорируйте такие сообщения. Настоящие сотрудники учреждений здравоохранения Республики Беларусь не уточняют данные пациентов через Telegram, WhatsApp и другие мессенджеры и не просят вводить коды подтверждения.

Рекомендация: При получении подобных сообщений просто игнорируйте их. Будьте особенно внимательны и предупреждайте пожилых родственников. Любые запросы на обновление медицинских данных должны поступать только официальным способом – лично в учреждении или через проверенные государственные сервисы.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ С «ОБНОВЛЕНИЕМ ДАННЫХ В МЕДКАРТЕ»



и другие мессенджеры

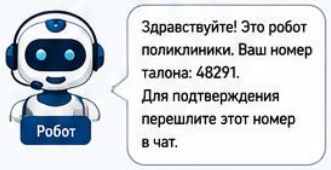
Мошенники активно рассылают сообщения в Telegram, WhatsApp и других мессенджерах от имени поликлиник, больниц и других учреждений здравоохранения.

Они просят «уточнить» или «обновить» персональные и медицинские данные для электронной медицинской карты: рост, вес, дату рождения, группу крови, хронические заболевания и другие сведения.

Для усиления давления мошенники используют предлог «медреформы» и пугают серьёзными последствиями: якобы без актуальной электронной карты человека не пустят на работу, в учебные заведения, не оформят ребёнка в сад/школу или не окажут медицинскую помощь.

КАК РАБОТАЕТ СХЕМА

1 Обещают «звонок от робота», который продиктует «номер талона» или код, и просят переслать его в чат.





Мошенник получает код и получает доступ к вашему аккаунту или госуслугам.

ИЛИ

2 Сразу просят ввести код подтверждения из SMS, пришедший на телефон.





Мошенник вводит код и получает доступ к вашему аккаунту или госуслугам.

В обоих случаях это позволяет злоумышленникам получить доступ к мессенджеру или аккаунту на государственном портале, после чего они могут похитить дополнительные данные, войти в банковские приложения или продолжить мошенничество от имени жертвы.

Схема рассчитана на доверие людей к медицинским учреждениям и страх перед возможными проблемами со здоровьем и документами.

КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ



1. НИКОГДА

не предоставляйте личные данные и не вводите коды из SMS по запросам из мессенджеров, даже если они приходят якобы от поликлиники или больницы.

2. ИГНОРИРУЙТЕ

такие сообщения. Настоящие сотрудники учреждений здравоохранения Республики Беларусь не уточняют данные пациентов через Telegram, WhatsApp и другие мессенджеры и не просят вводить коды подтверждения.



РЕКОМЕНДАЦИЯ

- При получении подобных сообщений просто игнорируйте их.
- Будьте особенно внимательны и предупреждайте пожилых родственников.
- Любые запросы на обновление медицинских данных должны поступать только официальным способом – лично в учреждении или через проверенные государственные сервисы.



БУДЬТЕ БДИТЕЛЬНЫ!
ЗАЩИТИТЕ СЕБЯ И СВОИХ БЛИЗКИХ!

Распознавание и предотвращение мошеннических схем с «сезонным отключением воды»

Мошенники массово рассылают SMS, сообщения в мессенджерах (Telegram, Viber и др.) и электронные письма якобы от имени «Водоканала», ЖКХ или управляющей компании. В сообщениях содержится информация о предстоящем графике отключения горячей воды в конкретном доме или районе с указанием точных дат и времени.

Для «удобства» жителей в сообщении размещена ссылка «Узнать подробнее», «Посмотреть график» или предложение перейти в чат-бот для уточнения информации.

Перейдя по ссылке, пользователь попадает на высококачественный поддельный сайт, который полностью имитирует официальный ресурс Водоканала или ЖКХ (аналогичный дизайн, логотипы, шрифты). На сайте просят:

ввести персональные данные (ФИО, адрес, номер телефона, паспортные данные);

«подтвердить личность» через МСИ (Межбанковскую систему идентификации);

авторизоваться через банковские данные или государственные сервисы.

В результате мошенники получают доступ к банковским аккаунтам, мессенджерам или Единому порталу электронных услуг. Дальше схема может развиваться по-разному: вымогательство денег, угрозы уголовной ответственности, оформление кредитов на жертву или продолжение целевого фишинга.

Схема особенно опасна в сезон плановых отключений горячей воды, когда люди действительно ожидают таких уведомлений и легче поддаются на провокацию.

Ключевые советы, чтобы не попадать в такую ситуацию:

Не переходите по ссылкам из сообщений об отключении воды. График отключений проверяйте только на официальных сайтах Водоканала, ЖКХ или местных исполнительных органов.

Никогда не вводите личные данные и не подтверждайте личность через подозрительные ссылки или чат-боты. Официальные организации не требуют этого по SMS, мессенджерам или неофициальным сайтам.

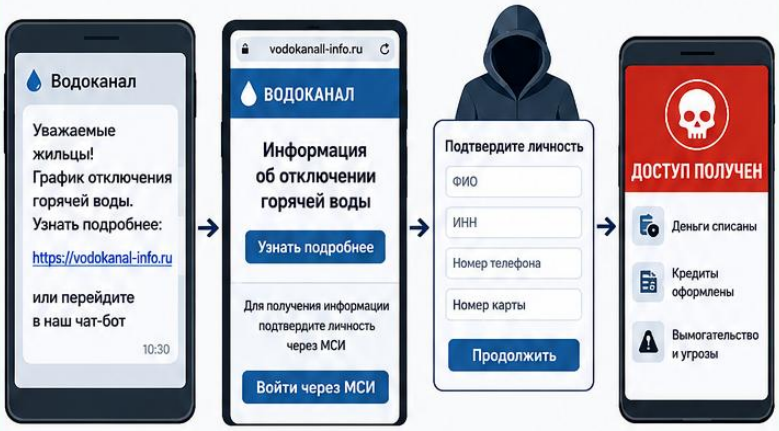
Рекомендация: При получении подобных уведомлений просто игнорируйте их и проверяйте информацию самостоятельно на проверенных государственных ресурсах. Это позволит избежать кражи доступа к банковским аккаунтам и финансовых потерь.

ОСТОРОЖНО: МОШЕННИКИ!

Сообщения о отключении горячей воды могут быть ловушкой



КАК РАБОТАЕТ СХЕМА



1. Вы получаете сообщение якобы от «Водоканала» или ЖКХ о графике отключения горячей воды со ссылкой или предложением перейти в чат-бот.
2. Вы переходите по ссылке и попадаете на поддельный сайт, имитирующий официальный ресурс Водоканала или ЖКХ.
3. Вас просят ввести личные данные или подтвердить личность через МСИ. Мошенники получают доступ к вашим банковским аккаунтам.
4. Дальше могут следовать вымогательство, угрозы или другие финансовые махинации.

КАК ЗАЩИТИТЬСЯ

Не переходите по ссылкам из сообщений об отключении воды.

График отключений проверяйте только на официальных сайтах Водоканала, ЖКХ или местных исполнительных органов.

Никогда не вводите личные данные и не подтверждайте личность

через подозрительные ссылки или чат-боты. Официальные организации не требуют этого по SMS, мессенджерам или неофициальным сайтам.

Сомневаетесь?

Позвоните в официальный контакт-центр Водоканала или ЖКХ по номеру с официального сайта и уточните информацию.

РЕКОМЕНДАЦИЯ:

При получении подобных уведомлений просто игнорируйте их и проверяйте информацию самостоятельно на проверенных государственных ресурсах. Это позволит избежать кражи доступа к банковским аккаунтам и финансовых потерь.



ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ ТОЛЬКО ЗДЕСЬ:

- ОФИЦИАЛЬНЫЙ САЙТ ВОДОКАНАЛА
- САЙТ ВАШЕГО ЖКХ
- ПОРТАЛ МЕСТНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ
- EGOV И ДРУГИЕ ГОСУДАРСТВЕННЫЕ РЕСУРСЫ

БУДЬТЕ БДИТЕЛЬНЫ!
ЗАЩИТИТЕ СЕБЯ И СВОИ ФИНАНСЫ!

Распознавание и предотвращение мошеннических схем с вовлечением подростков в противоправную деятельность

Мошенники целенаправленно работают в мессенджерах (Telegram, Discord, VK) и онлайн-играх (Brawl Stars, Roblox, Dota 2, Mobile Legends и др.). Они втираются в доверие к подросткам постепенно: начинают с дружеского общения, обсуждения игр, общих интересов, комплиментов и поддержки.

На первом этапе предлагают «простые и выгодные задания» – например, выполнить заказ в игре, протестировать аккаунт или помочь с покупкой. Затем просят перевести небольшую сумму денег якобы для покупки игровой валюты, скинов, бонусов, премиум-подписки или «совместной покупки» с обещанием вернуть больше.

После того, как подросток переводит деньги, схема резко меняется. Мошенники заявляют, что эти средства якобы были использованы для финансирования экстремистской, террористической или другой запрещённой деятельности. Далее следует мощное психологическое давление и шантаж:

Угрозы привлечения к уголовной ответственности (статьи о финансировании экстремизма);

Угрозы сообщить в милицию или родителям;

Угрозы опубликовать переписку, скриншоты, личные фото или видео в соцсетях.

Под предлогом «помочь решить проблему» и «замять дело» мошенники требуют новые, всё более крупные суммы денег. В некоторых случаях подростков склоняют к совершению противоправных действий (распространение запрещенного контента, вербовка других, переводы по чужим реквизитам и т.д.).

Схема рассчитана на недостаток жизненного опыта, страх перед наказанием и желание сохранить тайну от родителей.

Ключевые советы, чтобы не попадать в такую ситуацию:

Не переводите деньги незнакомцам в интернете, даже под предлогом покупки игровой валюты или помощи в игре. Обсуждайте все финансовые операции с родителями.

При появлении угроз, шантажа или требований денег – немедленно прекратите общение. Сохраните всю переписку (скриншоты, логи) и обратитесь к родителям и в правоохранительные органы.

Рекомендация: Родителям и сотрудникам рекомендуется регулярно проводить беседы с детьми и подростками о рисках общения с незнакомцами в сети. При возникновении подобной ситуации не пытайтесь «решить вопрос» самостоятельно – сразу обращайтесь в милицию. Своевременная реакция помогает пресечь мошенничество на ранней стадии.

ОНЛАЙН-ДРУЖБА МОЖЕТ СТАТЬ ЛОВУШКОЙ!

Мошенники втираются в доверие к подросткам
в мессенджерах и играх,
а затем шантажируют и вымогают деньги.

МЕССЕНДЖЕРЫ
Telegram Discord VK

ОНЛАЙН-ИГРЫ
Brawl Stars Roblox Dota 2 Mobile Legends и др.

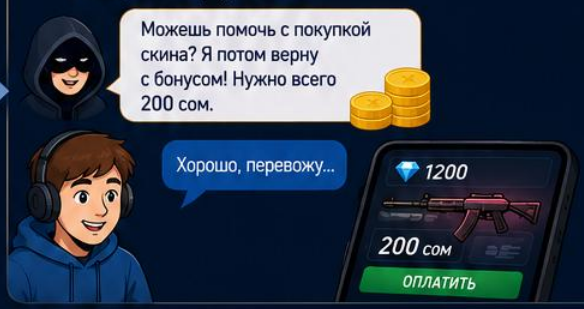
1 УСТАНОВЛЕНИЕ КОНТАКТА

Дружеское общение, обсуждение игр, общих интересов, комплименты, поддержка. Мошенник втирается в доверие.



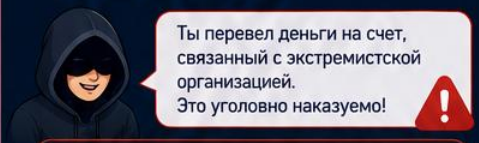
2 ПРОСЬБЫ О «ПРОСТЫХ ЗАДАНИЯХ»

Предлагают «выгодные задания», просят перевести небольшую сумму якобы для покупки валюты, скинов, бонусов, премиум-подписки или «совместной покупки» с обещанием вернуть больше.



3 ШАНТАЖ И УГРОЗЫ

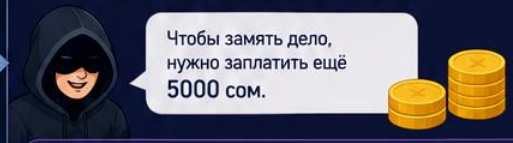
После перевода денег мошенники заявляют о «финансировании экстремизма» и начинают шантажировать.



- Угроза привлечения к уголовной ответственности (экстремизм)
- Угроза сообщить в милицию или родителям
- Угроза опубликовать переписку, скриншоты, личные фото/видео

4 ВЫМОГАТЕЛЬСТВО

Под предлогом «помочь решить проблему» требуют новые и всё более крупные суммы. Могут склонять к противоправным действиям.



- Требуют новые суммы денег
- Склоняют к противоправным действиям
- Используют страх и желание сохранить тайну

КАК ЗАЩИТИТЬСЯ

НИКОГДА НЕ ПЕРЕВОДИТЕ ДЕНЬГИ
незнакомым людям в интернете, даже если это «друг по игре». Все покупки делайте только через официальные магазины игр.

ПРИ УГРОЗАХ И ШАНТАЖЕ — НЕМЕДЛЕННО ПРЕКРАТИТЕ ОБЩЕНИЕ.
Сохраните переписку (скриншоты, логи) и сразу расскажите родителям или доверенному взрослому. Обратитесь в правоохранительные органы.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ?

1. Прекратите общение и не переводите деньги.
2. Сохраните все доказательства: скриншоты, логи чатов, реквизиты.
3. Расскажите родителям или доверенному взрослому.
4. Обратитесь в милицию.



102 милиция

РОДИТЕЛЯМ И СОТРУДНИКАМ РЕКОМЕНДУЕТСЯ

- Регулярно говорите с детьми о рисках в интернете.
- Объясняйте, что настоящие друзья не просят денег и не угрожают.
- Поддерживайте доверительные отношения с подростком.
- При возникновении проблемы не пытайтесь «решить вопрос» самостоятельно – обращайтесь за помощью к родителям и в милицию.



РЕКОМЕНДАЦИЯ:

При получении подобных уведомлений просто игнорируйте их и проверяйте информацию самостоятельно на проверенных государственных ресурсах. Это позволит избежать кражи доступа к банковским аккаунтам и финансовых потерь.



ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ ТОЛЬКО ЗДЕСЬ:

- Официальный сайт Водоканала
- Сайт вашего ЖКХ
- Портал местных исполнительных органов
- eGov и другие государственные ресурсы

НЕ ДАЙ СЕБОЙ МАНИПУЛИРОВАТЬ!
ДОВЕРЯЙ, НО ПРОВЕРЯЙ! БУДЬ БДИТЕЛЕН В СЕТИ!

Распознавание и предотвращение вербовки

Вербовщики редко начинают с прямых призывов к противоправным действиям. Они действуют постепенно и очень профессионально, используя мессенджеры (Telegram, Discord), социальные сети и онлайн-игры.

Сначала вербовщик входит в доверие: проявляет интерес к жизни человека, поддерживает в разговорах, делает комплименты, предлагает «дружбу». Он может обещать деньги, материальную помощь, эмоциональную поддержку, внимание и чувство собственной значимости («ты особенный», «только ты можешь это сделать», «мы тебя понимаем»).

Со временем вербовщик начинает психологически обрабатывать жертву:

Убеждает, что родители, друзья или близкие «не понимают» его, «не ценят» или «мешают развиваться».

Создаёт ощущение избранности и исключительности («ты не такой, как все»).

Постепенно появляются странные просьбы: выполнить «невинное» задание, передать какую-то информацию, встретиться «просто поговорить», сделать звонок или переслать фото/документы.

Используется давление на чувство вины, долга, обиды или мести («если ты настоящий друг – помоги», «они к тебе несправедливы»).

На финальных этапах человека могут втянуть в противоправную деятельность: распространение запрещённого контента, участие в акциях, сбор информации, вербовку других людей, финансовые операции или даже более серьёзные преступления. Весь процесс построен на манипуляции эмоциями и постепенном повышении уровня требований.

Ключевые советы, чтобы не попадать в такую ситуацию:

Настораживайтесь, если новый знакомый слишком быстро становится «самым близким» и предлагает особые отношения, деньги или поддержку без явных причин.

Не соглашайтесь на встречи, просьбы или действия, смысл которых вам не объясняют, а также не передавайте деньги, вещи, документы или информацию незнакомым людям.

Рекомендация: При появлении давления, запугивания или просьб молчать – немедленно прервите общение, сохраните переписку и обратитесь в правоохранительные органы. Не пытайтесь разобраться самостоятельно. Лучшая защита – своевременное обращение за помощью.

ВЕРБОВКА – ЭТО НЕ ВСЕГДА ПРЯМЫЕ ПРИЗЫВЫ!

Вербовщики действуют постепенно, используя доверие и манипуляции.

ГДЕ ДЕЙСТВУЮТ ВЕРБОВЩИКИ?

Telegram · Discord · Социальные сети · Онлайн-игры

1. УСТАНОВЛЕНИЕ КОНТАКТА

Вербовщик входит в доверие: проявляет интерес, поддерживает, делает комплименты, предлагает «дружбу».



Обещания: деньги, помощь, поддержка, внимание, значимость. «Ты особенный», «Только ты можешь это сделать».

2. ПСИХОЛОГИЧЕСКАЯ ОБРАБОТКА

Вербовщик внушает нужные мысли и формирует зависимость.

- Убеждает, что близкие «не понимают», «мешают развиваться».
- Создаёт ощущение избранности и исключительности: «ты не такой, как все».
- Использует чувство вины, долга, обиды или мести: «если ты настоящий друг — помоги».



3. ПРОСЬБЫ И «НЕВИННЫЕ» ЗАДАНИЯ

Появляются странные просьбы, которые кажутся безобидными.

- Передать какую-то информацию
- Сделать звонок или переслать сообщение
- Встретиться «просто поговорить»
- Переслать фото/документы
- Выполнить «простое задание»



4. ВТЯГИВАНИЕ В ДЕЯТЕЛЬНОСТЬ

Постепенно требования становятся серьёзнее и опаснее.

- Распространение запрещённого контента
- Участие в акциях, провокациях
- Сбор и передача информации
- Вербовка других людей
- Финансовые операции
- Более серьёзные преступления

Весь процесс построен на манипуляции эмоциями и постепенном повышении уровня требований.

ПОМНИ!

Вербовщики играют на твоих эмоциях, страхах, обидах и желании быть важным.



Не дай себя использовать!

КАК НЕ ПОПАСТЬ В ЛОВУШКУ?

НАСТОРАЖИВАЙТЕСЬ, ЕСЛИ:

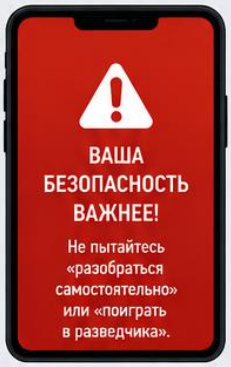
- новый знакомый слишком быстро становится «лучшим другом»;
- предлагает особые отношения, деньги, поддержку или внимание без видимых причин;
- пытается изолировать вас от друзей и близких.

НЕ СОГЛАШАЙТЕСЬ НА:

- странные просьбы;
- тайные встречи;
- передачу денег, документов или информации;
- задания, смысл которых вам не объясняют или объясняют туманно.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ЧУВСТВУЕТЕ УГРОЗУ?

- Немедленно прекратите общение.
- Сохраните всю переписку (скриншоты, логи).
- Обратитесь к родным или доверенному взрослому.
- Сообщите в правоохранительные органы.



РОДИТЕЛЯМ И ПЕДАГОГАМ

- Регулярно разговаривайте с детьми о рисках в интернете.
- Объясняйте, что настоящие друзья не манипулируют, не просят тайны и не вовлекают в незаконные действия.
- Поддерживайте доверительные отношения и будьте внимательны к изменениям в поведении ребёнка.



ЛУЧШАЯ ЗАЩИТА – ЭТО БДИТЕЛЬНОСТЬ, КРИТИЧЕСКОЕ МЫШЛЕНИЕ И СВОЕВРЕМЕННОЕ ОБРАЩЕНИЕ ЗА ПОМОЩЬЮ!

102

Распознавание и предотвращение мошеннических схем с «сотрудниками МЧС»

Мошенники активно обзванивают граждан по телефону, представляясь работниками Министерства по чрезвычайным ситуациям (МЧС), пожарной инспекции или сотрудниками отдела профилактики.

Они настойчиво утверждают, что в квартире или частном доме необходимо срочно установить огнетушители, автономные пожарные извещатели (датчики дыма) или другие средства пожаротушения. Мошенники ссылаются на якобы новые требования законодательства и угрожают крупными штрафами (от нескольких сотен до тысяч рублей), административной ответственностью или даже принудительной проверкой с выездом на место.

Для «оформления» или «оплаты» они могут:

Запрашивать паспортные данные;

Просить реквизиты банковской карты;

Требовать коды из SMS;

Предлагать перейти по ссылке для оплаты или оформления заказа.

В некоторых случаях мошенники приезжают на адрес с «огнетушителями» по завышенной цене и пытаются получить наличные или данные карты на месте.

Схема построена на страхе людей перед пожаром, уважении к службе МЧС и желании избежать штрафов. Особенно часто страдают пожилые граждане.

Ключевые советы, чтобы не попадать в такую ситуацию:

Помните, что МЧС не продаёт огнетушители и средства пожаротушения и не звонит гражданам с требованиями что-либо купить или установить.

Никогда не передавайте по телефону паспортные данные, реквизиты банковских карт или коды из SMS, даже если звонят якобы из МЧС.

Рекомендация: При подобных звонках сразу прекращайте разговор и не выполняйте никаких требований. Информацию о проверках пожарной безопасности проверяйте только через официальные каналы МЧС. Особенно предупредите пожилых родственников.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ С «СОТРУДНИКАМИ МЧС»





Мошенники активно обзванивают граждан по телефону, **представляясь работниками МЧС**, пожарной инспекции или сотрудниками отдела профилактики.

Они настойчиво утверждают, что в квартире или частном доме необходимо срочно установить огнетушители, автономные пожарные извещатели (датчики дыма) или другие средства пожаротушения. Мошенники ссылаются на якобы новые требования законодательства и угрожают крупными штрафами (от нескольких сотен до тысяч рублей), административной ответственностью или даже принудительной проверкой с выездом на место.



ДЛЯ «ОФОРМЛЕНИЯ» ИЛИ «ОПЛАТЫ» ОНИ МОГУТ:



Запрашивать паспортные данные



Просить реквизиты банковской карты



Требовать коды из SMS



Предлагать перейти по ссылке для оплаты или оформления заказа



В некоторых случаях мошенники приезжают на адрес с «огнетушителями» по завышенной цене и пытаются получить наличные или данные карты на месте.

Схема построена на страхе людей перед пожаром, уважении к службе МЧС и желании избежать штрафов. Особенно часто страдают пожилые граждане.

КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ:



ПОМНИТЕ: МЧС **не продаёт** огнетушители и средства пожаротушения и **не звонит** гражданам с требованиями что-либо купить или установить.



НИКОГДА не передавайте по телефону паспортные данные, реквизиты банковских карт или коды из SMS, даже если звонят якобы из МЧС.

РЕКОМЕНДАЦИЯ: При подобных звонках сразу прекращайте разговор и не выполняйте никаких требований. Информацию о проверках пожарной безопасности проверяйте **только через официальные каналы МЧС.**

ОФИЦИАЛЬНЫЕ КАНАЛЫ МЧС:

Официальный сайт
mchs.gov.by

Телефон для справок
101

Обращайтесь в районные (городские) отделы по чрезвычайным ситуациям

Будьте бдительны! Проверяйте информацию, предупредите близких и не дайте мошенникам шанса!

Распознавание и предотвращение мошеннических схем с поддельными чеками о покупках

Мошенники массово рассылают на электронную почту поддельные квитанции, чеки и уведомления якобы от популярных маркетплейсов (Ozon, Wildberries, Yandex.Market, AliExpress и других).

В письме используется официальный стиль оформления: логотипы, номера заказов, суммы и даты. В нём сообщается об «неизвестной транзакции», «случайном заказе», «ошибочном платеже» или «подозрительной покупке», которую нужно срочно отменить, чтобы деньги не списались. Для удобства в письме размещена кнопка или ссылка «Отменить заказ», «Оформить возврат» или «Проверить транзакцию».

Перейдя по ссылке, пользователь попадает на высококачественный фишинговый сайт, который идеально имитирует интерфейс маркетплейса или банка. На сайте открывается форма возврата средств, где просят ввести данные банковской карты:

Номер карты;

Срок действия;

CVV/CVC-код;

Иногда имя держателя и другие сведения.

После ввода данных мошенники мгновенно получают доступ к карте и списывают деньги. В дальнейшем украденные данные могут использоваться для других покупок, оформления микрозаймов или продажи в даркнете.

Схема особенно эффективна, потому что многие люди действительно делают покупки на маркетплейсах и ожидают уведомлений по почте. Мошенники часто используют реальные данные о прошлых заказах жертвы (утечки баз данных), чтобы письмо выглядело правдоподобно.

Ключевые советы, чтобы не попадать в такую ситуацию:

Не переходите по ссылкам из подозрительных писем о покупках, транзакциях или отмене платежей. Все операции проверяйте только в официальном приложении или на сайте маркетплейса.

Никогда не вводите данные банковской карты на сайтах, к которым перешли по ссылке из письма. Проверяйте адрес отправителя – часто в нём есть лишние или изменённые символы.

Рекомендация: При получении подобных писем просто удаляйте их. Если сомневаетесь в какой-либо транзакции – заходите в личный кабинет самостоятельно, а не по ссылкам из почты. Это надёжный способ защитить свои средства.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ

С ПОДДЕЛЬНЫМИ ЧЕКАМИ О ПОКУПКАХ





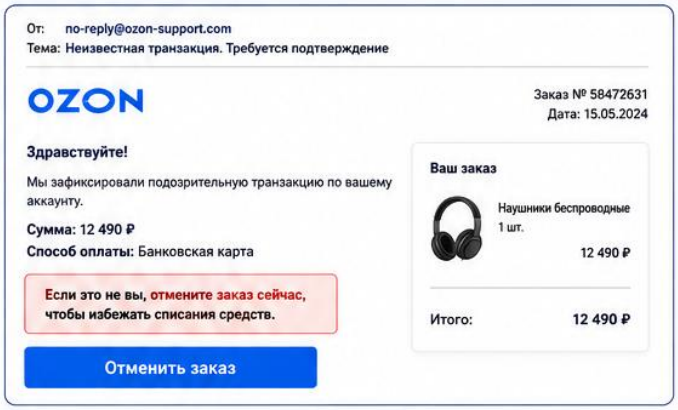
OZON WILDBERRIES Яндекс Маркет AliExpress

Мошенники массово рассылают на электронную почту поддельные квитанции, чеки и уведомления якобы от популярных маркетплейсов (Ozon, Wildberries, Yandex.Market, AliExpress и других).



В письме используется официальный стиль оформления: логотипы, номера заказов, суммы и даты. В нём сообщается об «неизвестной транзакции», «случайном заказе», «ошибочном платеже» или «подозрительной покупке», которую нужно срочно отменить, чтобы деньги не списались.

Для удобства в письме размещена кнопка или ссылка «Отменить заказ», «Оформить возврат» или «Проверить транзакцию».

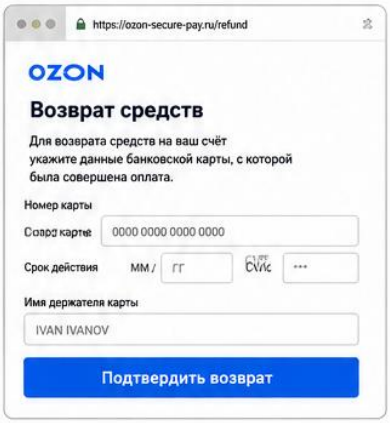




Перейдя по ссылке, пользователь попадает на высококачественный фишинговый сайт, который идеально имитирует интерфейс маркетплейса или банка.

На сайте открывается форма возврата средств, где просят ввести данные банковской карты:

- Номер карты
- Срок действия
- CVV/CVC-код
- Иногда имя держателя и другие сведения.



ВАЖНО!

После ввода данных мошенники мгновенно получают доступ к карте и списывают деньги.



В дальнейшем украденные данные могут использоваться для других покупок, оформления микрозаймов или продажи в даркнете.



Схема особенно эффективна, потому что многие люди действительно делают покупки на маркетплейсах и ожидают уведомлений по почте. Мошенники часто используют реальные данные о прошлых заказах жертвы (утечки баз данных), чтобы письмо выглядело правдоподобно.

ПРИЗНАКИ ПОДОЗРИТЕЛЬНОГО ПИСЬМА

- Неожиданное письмо о заказе или платеже
- Срочные требования и угрозы списания денег
- Ссылка ведёт не на официальный сайт
- Адрес отправителя похож на настоящий, но содержит ошибку или лишние символы



КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ:



НЕ ПЕРЕХОДИТЕ по ссылкам из подозрительных писем о покупках, транзакциях или отмене платежей.

Все операции проверяйте только в официальном приложении или на сайте маркетплейса.



НИКОГДА не вводите данные банковской карты на сайтах, к которым перешли по ссылке из письма.

Проверяйте адрес отправителя – часто в нём есть лишние или изменённые символы.



ПРОВЕРЯЙТЕ информацию только через официальные каналы.

Официальные маркетплейсы никогда не запрашивают данные карты по электронной почте.



РЕКОМЕНДАЦИЯ:

При получении подобных писем просто удаляйте их.
Если сомневаетесь в какой-либо транзакции – заходите в личный кабинет самостоятельно, а не по ссылкам из почты. Это надёжный способ защитить свои средства.



Распознавание и предотвращение мошеннических схем с «работой» по размещению карточек товаров

Мошенники размещают в интернете (в Telegram-каналах, группах по поиску работы, Kufar, VK и других площадках) объявления о простой и высокооплачиваемой подработке. Предлагается «лёгкая удалённая работа»: размещать карточки товаров на досках объявлений, интернет-магазинах или маркетплейсах и передавать контакты потенциальных покупателей «работодателю».

На первом этапе всё выглядит легально: дают инструкции, шаблоны объявлений, небольшую тестовую оплату. Человек использует свой личный номер телефона, аккаунт на сайте объявлений или почту для регистрации и работы.

На деле это один из способов создания «чистых» аккаунтов. Мошеннические колл-центры используют эти аккаунты для публикации фейковых объявлений о продаже товаров, автомобилей, квартир и т.д. Когда аккаунт «наработает» репутацию и начинает активно использоваться в крупных мошеннических схемах, его блокируют администрацией площадки.

В результате «сотрудник» остаётся без обещанной оплаты, вся переписка с покупателями исчезает, а на его номер или аккаунт начинают поступать жалобы и претензии от обманутых людей. Иногда такие аккаунты позже используются для более серьёзных преступлений, что может создать проблемы с правоохранительными органами.

Схема рассчитана на студентов, пенсионеров, домохозяек и всех, кто ищет лёгкий дополнительный заработок.

Ключевые советы, чтобы не попадать в такую ситуацию:

Избегайте «лёгких» вакансий, где требуется размещать объявления и передавать контакты покупателей незнакомому «работодателю».

Не используйте свои личные номера телефонов, аккаунты и данные для сомнительной удалённой работы.

Рекомендация: Любые предложения быстрого заработка с минимальными усилиями и передачей контактов – это сигнал к повышенному вниманию. Перед соглашением на такую «работу» тщательно проверяйте работодателя через официальные источники. Не рискуйте своей репутацией и безопасностью.

ОСТОРОЖНО! МОШЕННИЧЕСКИЕ СХЕМЫ С «РАБОТОЙ» ПО РАЗМЕЩЕНИЮ КАРТОЧЕК ТОВАРОВ

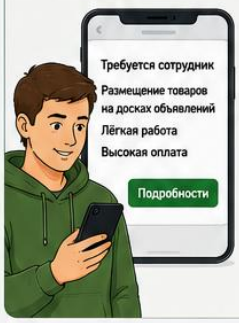
Республика Беларусь

Мошенники предлагают «лёгкую» и «высокооплачиваемую» подработку: размещать карточки товаров на досках объявлений, интернет-магазинах или маркетплейсах и передавать контакты покупателей «работодателю».

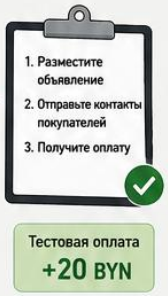
Telegram Kufar ВКонтакте и другие

КАК РАБОТАЕТ СХЕМА

1. Вы видите объявление о простой и высокооплачиваемой подработке.



2. Вам дают инструкции, шаблоны объявлений и небольшую тестовую оплату.



Тестовая оплата +20 BYN

3. Вы используете свой номер телефона, аккаунт на сайте объявлений или почту для работы.



4. Вы размещаете карточки товаров и передаёте контакты потенциальных покупателей «работодателю».



5. Вам обещают стабильный доход и долгосрочное сотрудничество.



- Стабильный доход
- Бонусы
- Премии
- Карьерный рост

ЧТО ПРОИСХОДИТ НА САМОМ ДЕЛЕ

1. Ваш аккаунт – это «чистая» страница. Мошеннические колл-центры используют его для публикации фейковых объявлений (товары, авто, квартиры и т.д.).



2. Когда аккаунт «наработает» репутацию, его начинают активно использовать в крупных мошеннических схемах.



3. Аккаунт блокируют администрацией площадки.



4. Вы остаётесь без оплаты, теряете переписку, а на вас поступают жалобы и претензии от обманутых людей. Такие аккаунты могут использоваться для более серьёзных преступлений.



НА КОГО РАССЧИТАНА СХЕМА?

На студентов, пенсионеров, домохозяек и всех, кто ищет лёгкий дополнительный заработок.

ИТОГ:

Потеря времени, денег, репутации и возможные проблемы с законом.

КАК НЕ ПОПАСТЬ В ТАКУЮ СИТУАЦИЮ?

ИЗБЕГАЙТЕ
«лёгких» вакансий, где требуется размещать объявления и передавать контакты покупателей незнакомому «работодателю».

НЕ ИСПОЛЬЗУЙТЕ
свои личные номера телефонов, аккаунты и данные для сомнительной удалённой работы.

ПРОВЕРЯЙТЕ
работодателя через официальные источники: сайт компании, отзывы, госреестры, контакты.
Не ведитесь на красивые обещания и быстрые выплаты!

РЕКОМЕНДАЦИЯ:

Любые предложения быстрого заработка с минимальными усилиями и передачей контактов – это сигнал к повышенному вниманию. Перед соглашением на такую «работу» тщательно проверяйте работодателя через официальные источники.

НЕ РИСКУЙТЕ СВОЕЙ РЕПУТАЦИЕЙ И БЕЗОПАСНОСТЬЮ!
БУДЬТЕ БДИТЕЛЬНЫ!

Распознавание и предотвращение мошеннических схем с «сотрудниками налоговой инспекции»

Мошенники всё чаще обзванивают граждан, представляясь сотрудниками Министерства по налогам и сборам (МНС) Республики Беларусь, налоговой инспекции или «отделом камеральных проверок».

Они сообщают о якобы выявленных нарушениях: неуплаченных налогах, ошибках в декларации, переплате или необходимости срочного «декларирования доходов». Для создания правдоподобности называют фамилию, должность и даже номер якобы постановления. Мошенники создают сильное ощущение срочности и угрозы: «если не оплатить сегодня – будет крупный штраф», «счёт будет заблокирован», «возбудят административное или уголовное дело».

В ходе разговора они требуют:

Код из SMS (якобы «для подтверждения личности»);

Паспортные данные;

Реквизиты банковской карты (номер, срок действия, CVV);

Перейти по ссылке для оплаты «налога» или «штрафа»;

Установить приложение для «подачи декларации»;

Оплатить «недоимку» через отправленную ссылку или QR-код.

После получения данных или доступа к банковским приложениям мошенники списывают деньги. В некоторых случаях используют полученную информацию для оформления кредитов и микрозаймов на имя жертвы.

Схема построена на страхе перед государственными органами, недостаточной налоговой грамотности и психологическом давлении. Особенно часто жертвами становятся пожилые люди и предприниматели.

Ключевые советы, чтобы не попадать в такую ситуацию:

Настоящие сотрудники МНС никогда не запрашивают по телефону коды из SMS, паспортные данные, реквизиты карт, не просят переходить по ссылкам или устанавливать приложения.

При любом звонке с требованием срочно оплатить «налог» или «декларировать» деньги – немедленно прекратите разговор. Декларирование – это подача декларации, а не передача наличных или переводы третьим лицам.

Рекомендация: Проверяйте любую информацию только на официальных сайтах МНС. Не сообщайте личные данные и не выполняйте инструкции звонившего. Особенно предупредите пожилых родственников и близких. При подозрении – обращайтесь в милицию.

ОСТОРОЖНО! МОШЕННИЧЕСКИЕ СХЕМЫ С «СОТРУДНИКАМИ НАЛОГОВОЙ ИНСПЕКЦИИ»

Министерство по налогам и сборам Республики Беларусь

Мошенники представляются сотрудниками Министерства по налогам и сборам (МНС) Республики Беларусь или налоговой инспекции и выманивают личные данные и деньги.

КАК РАБОТАЕТ СХЕМА

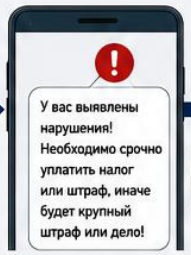
1 Звонок от мошенника

Мошенник звонит и представляется сотрудником МНС, налоговой инспекции или «отдела камеральных проверок».



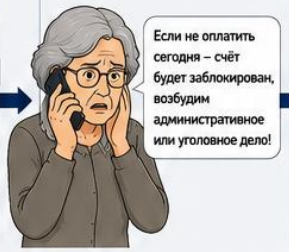
2 Сообщение о нарушении

Сообщает о якобы выявленных нарушениях, неуплаченных налогах, ошибках в декларации, переплате и т.д.



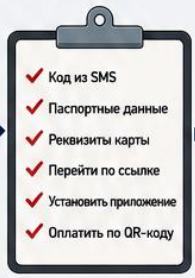
3 Создание срочности и давления

Называет ваши данные, должность и № якобы постановления. Создаёт ощущение угрозы.



4 Требование данных и действий

Просит предоставить данные или выполнить действия для «решения вопроса».



5 Похищение денег и данных

Получив данные или доступ к приложениям, мошенники списывают деньги или берут кредиты на имя жертвы.



ЧТО ТРЕБУЮТ МОШЕННИКИ



Код из SMS (якобы «для подтверждения личности»)



Паспортные данные



Реквизиты банковской карты (номер, срок действия, CVV)



Перейти по ссылке для оплаты «налога» или «штрафа»



Установить приложение для «подачи декларации»



Оплатить «недоимку» через ссылку или QR-код

ЧЕМ ЭТО ОПАСНО?

- Списывают деньги с банковских карт и счетов
- Используют данные для оформления кредитов и микрозаймов
- Похищают личные данные и используют их в других схемах
- Могут наступить административная и уголовная ответственность



МНС НИКОГДА НЕ:

- запрашивает коды из SMS по телефону
- просит паспортные данные и реквизиты карт
- просит переходить по ссылкам или устанавливать приложения
- требует оплачивать налоги или штрафы по телефону

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ?



1. Прекратите разговор!

При любом звонке с требованием оплатить «налог», «штраф» или «декларировать» деньги – немедленно прекратите разговор.

Декларирование – это подача декларации, а не передача наличных или переводы третьим лицам!



2. Не сообщайте данные!

Не сообщайте никому по телефону коды из SMS, паспортные данные, реквизиты карт и другую конфиденциальную информацию.

Настоящие сотрудники МНС никогда не запрашивают такие данные по телефону.



3. Проверяйте информацию!

Проверяйте любую информацию только на официальном сайте МНС: mns.gov.by или лично в инспекции.

РЕКОМЕНДАЦИЯ!



- Проверяйте информацию только на официальных сайтах МНС.
- Не сообщайте личные данные и не выполняйте инструкции звонившего.
- Особенно предупредите пожилых родственников и близких.
- При подозрении на мошенничество – обращайтесь в милицию по телефону 102.

БУДЬТЕ БДИТЕЛЬНЫ! ЗАЩИТИТЕ СВОИ ДЕНЬГИ И ЛИЧНЫЕ ДАННЫЕ!

Распознавание и предотвращение мошеннических схем с «работой» по размещению карточек товаров

Мошенники активно публикуют объявления о «лёгкой подработке» в Telegram-каналах, группах ВКонтакте, Kufar, в чатах по поиску работы и других площадках. Предлагается простая удалённая работа без опыта: размещать готовые карточки товаров (телефоны, бытовая техника, автомобили и т.д.) на популярных досках объявлений, маркетплейсах или в соцсетях и пересылать контакты заинтересованных покупателей «работодателю».

На начальном этапе схема выглядит вполне безобидно:

Выдают подробные инструкции и шаблоны объявлений;

Могут даже заплатить небольшую тестовую сумму, чтобы вызвать доверие;

Просят зарегистрироваться на площадке с помощью своего личного номера телефона, аккаунта или электронной почты.

На деле это отработанный способ создания «чистых» аккаунтов для мошеннических колл-центров. После того, как аккаунт набирает определённую активность и положительную историю, его начинают использовать для публикации фейковых объявлений о продаже товаров по заниженным ценам, автомобилей, квартир и других дорогих вещей.

Когда аккаунт «засветился» и на него поступает много жалоб от обманутых людей, администрация площадки блокирует его. В результате человек, согласившийся на «работу», остаётся без обещанной зарплаты, теряет доступ к своему аккаунту, а вся переписка с покупателями исчезает. Кроме того, на его личный номер телефона или почту начинают приходить претензии, угрозы и жалобы от пострадавших.

В некоторых случаях такие аккаунты используются для более серьёзных преступлений, что может создать проблемы с правоохранительными органами для ничего не подозревающего «сотрудника».

Схема особенно привлекательна для студентов, пенсионеров, мам в декрете и всех, кто ищет простой дополнительный заработок.

Ключевые советы, чтобы не попадать в такую ситуацию:

Любые «лёгкие» вакансии с передачей контактов покупателей – это красный флаг. Избегайте таких предложений.

Не используйте свои личные номера телефонов, аккаунты и данные для сомнительной удалённой работы.

Рекомендация: Мошенники постоянно ищут новых «помощников». Перед соглашением на любую подработку тщательно проверяйте работодателя. Не рискуйте своей репутацией и безопасностью – лучше отказаться от сомнительных предложений.

ОСТОРОЖНО! МОШЕННИЧЕСКИЕ СХЕМЫ С «РАБОТОЙ» ПО РАЗМЕЩЕНИЮ КАРТОЧЕК ТОВАРОВ

Республика Беларусь

Мошенники предлагают «лёгкую подработку»: размещать карточки товаров на досках объявлений, маркетплейсах или в соцсетях и передавать контакты покупателей «работодателю».

Где ищут «сотрудников»?

Telegram · ВКонтакте · Kufar · Чаты по поиску работы и др.

КАК РАБОТАЕТ СХЕМА

1 Привлекательное предложение

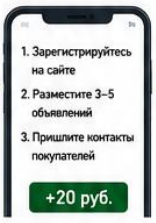
«Лёгкая работа» без опыта, высокий доход, свободный график.



Цель – заинтересовать и вызвать доверие.

2 Инструкции и тестовая оплата

- Выдают инструкции и шаблоны объявлений.
- Могут заплатить небольшую сумму за «тестовое задание».



Цель – убедить, что работа легальная.

3 Регистрация с вашими данными

Просят зарегистрироваться на площадке с помощью вашего номера телефона, аккаунта или e-mail.



Цель – получить доступ к вашим личным данным и аккаунтам.

4 Создание «чистых» аккаунтов

Ваш аккаунт набирает активность и положительную историю.



Цель – подготовить аккаунт для преступных схем.

5 Использование для мошенничества

На аккаунте публикуют фейковые объявления о продаже товаров по заниженным ценам.



Цель – обмануть как можно больше людей.

6 Блокировка аккаунта и проблемы для вас

На аккаунт поступает много жалоб – его блокируют.



- Нет доступа к аккаунту
- Нет обещанной оплаты
- Переписка исчезает
- Жалобы и претензии

Цель – уйти от ответственности, оставив вас крайним.

ЧЕМ ЭТО ОПАСНО ДЛЯ ВАС?

Потеря денег и времени

Вас обманывают – обещанную зарплату вы не получите.



Блокировка аккаунта

Вы теряете доступ к своему аккаунту и всей переписке.



Жалобы и угрозы

На ваш номер телефона или почту приходят жалобы, угрозы и претензии от обманутых людей.



Риск серьёзных последствий

Ваши данные могут быть использованы для более серьёзных преступлений, что может привести к проблемам с законом.



Репутационные риски

Ваши действия могут навредить вашей репутации и отношениям с окружающими.



КАК НЕ ПОПАСТЬСЯ НА УЛОВКУ МОШЕННИКОВ?

1 «Лёгкие» вакансии – красный флаг

Любые предложения с лёгким заработком и передачей контактов покупателей – это признак мошенничества.



Будьте бдительны!

2 Не используйте свои личные данные

Не используйте свои личные номера телефонов, аккаунты, почту и другие данные для сомнительной работы.



3 Проверяйте работодателя

Перед тем как соглашаться на работу, проверяйте информацию о работодателе: отзывы, контакты, официальные сайты. Не доверяйте незнакомцам!



4 Не передавайте контакты покупателей

Передача контактов третьим лицам может быть использована для мошенничества.



РЕКОМЕНДАЦИЯ

Мошенники постоянно ищут новых «помощников». Перед соглашением на любую подработку тщательно проверяйте работодателя. Не рискуйте своей репутацией и безопасностью – лучше отказаться от сомнительных предложений.

Если предложение кажется слишком хорошим, чтобы быть правдой — скорее всего, это обман!



ЗАЩИТИТЕ СЕБЯ И СВОИ ДАННЫЕ!

- Думайте критически
- Проверяйте информацию
- Не передавайте личные данные
- Остерегайтесь заманчивых предложений

При подозрении на мошенничество обращайтесь в милицию **102**

Распознавание и предотвращение мошеннических схем с ИИ-клонированием голоса

Мошенники активно используют современные нейросети (голосовые клоны на базе ИИ) для создания очень реалистичных аудиосообщений. Они копируют голос ваших близких – ребёнка, супруга, родителей, друзей или других родственников.

Схема обычно работает следующим образом:

Мошенники взламывают аккаунт одного из ваших контактов (Telegram, WhatsApp, Viber) или используют поддельный номер.

Жертве приходит голосовое сообщение якобы от реального человека. Голос звучит очень естественно – с характерными интонациями, эмоциями, дыханием и даже привычными словечками.

В сообщении звучит срочная просьба: «Мам, одолжи денег…», «Пап, срочно переведи на карту», «Мне нужна помощь, я в беде» и т.д. Часто указывается конкретная сумма и причина (попал в аварию, телефон сел, потерял деньги и т.п.).

Эмоциональное давление очень сильное – человек слышит родной голос в стрессовой ситуации и склонен действовать быстро, без дополнительной проверки. После перевода денег мошенники могут продолжить общение, чтобы выманить ещё больше.

Такие атаки стали особенно распространены в 2025–2026 годах благодаря доступности ИИ-инструментов для клонирования голоса по нескольким секундам оригинальной записи.

Ключевые советы, чтобы не попадать в такую ситуацию:

Никогда не переводите деньги сразу после получения голосового сообщения с просьбой о финансовой помощи, даже если голос полностью совпадает с голосом близкого человека.

Всегда проверяйте информацию альтернативным способом – перезвоните человеку по другому номеру или напишите в другой мессенджер/канал связи.

Рекомендация: В 2026 году это одно из главных правил цифровой безопасности: при любой срочной просьбе о деньгах по голосу или тексту – обязательная независимая проверка. Предупредите близких, особенно пожилых родственников.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ С ИИ-КЛОНИРОВАНИЕМ ГОЛОСА

БЕРЕГИТЕ СЕБЯ И СВОИХ БЛИЗКИХ!

Мошенники активно используют современные нейросети (голосовые клоны на базе ИИ) для создания очень реалистичных аудиосообщений. Они копируют голос ваших близких – ребёнка, супруга, родителей, друзей или других родственников.

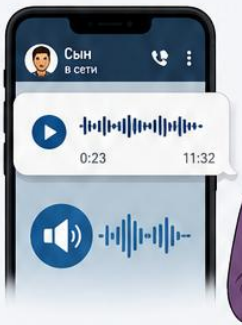


КАК РАБОТАЕТ СХЕМА?

1. Мошенники взламывают аккаунт одного из ваших контактов (Telegram, WhatsApp, Viber) или используют поддельный номер.



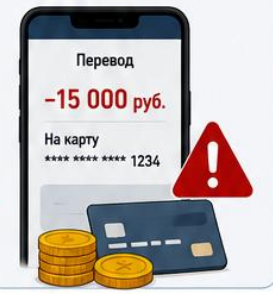
2. Жертве приходит голосовое сообщение якобы от реального человека. Голос звучит очень естественно – с характерными интонациями, эмоциями, дыханием и даже привычными словечками.



3. В сообщении звучит срочная просьба: «Мам, одолжи денег...», «Пап, срочно переведи на карту», «Мне нужна помощь, я в беде» и т.д. Часто указывается конкретная сумма и причина (попал в аварию, телефон сел, потерял деньги и т.п.).



4. Эмоциональное давление очень сильное – человек слышит родной голос в стрессовой ситуации и склонен действовать быстро, без дополнительной проверки. После перевода денег мошенники могут продолжить общение, чтобы выманить ещё больше.



Такие атаки стали особенно распространены в 2025–2026 годах благодаря доступности ИИ-инструментов для клонирования голоса по нескольким секундам оригинальной записи.



2025–2026
БУДЬТЕ БДИТЕЛЬНЫ!

КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ:



1. НИКОГДА НЕ ПЕРЕВОДИТЕ ДЕНЬГИ

сразу после получения голосового сообщения с просьбой о финансовой помощи, даже если голос полностью совпадает с голосом близкого человека.



2. ВСЕГДА ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ АЛЬТЕРНАТИВНЫМ СПОСОБОМ

перезвоните человеку по другому номеру или напишите в другой мессенджер/канал связи.

РЕКОМЕНДАЦИЯ

В 2026 году это одно из главных правил цифровой безопасности: при любой срочной просьбе о деньгах по голосу или тексту – обязательная независимая проверка.



Предупредите близких, особенно пожилых родственников.

ПОМНИТЕ! МОШЕННИКИ ИСПОЛЬЗУЮТ ДОВЕРИЕ И ЭМОЦИИ. ПРОВЕРЯЙТЕ – ЭТО ЗАЩИТИТ ВАС И ВАШИХ БЛИЗКИХ!

102
В СЛУЧАЕ ПОДОЗРЕНИЯ – ОБРАЩАЙТЕСЬ В МИЛИЦИЮ

Распознавание и предотвращение мошенничества с помощью старых объявлений

Мошенники регулярно мониторят доски объявлений (Kufar и другие) и находят старые, давно закрытые объявления о продаже товаров, услуг, автомобилей, недвижимости и т.д.

Они пишут потенциальной жертве как обычные заинтересованные покупатели: «Здравствуйте, объявление ещё актуально?», «Можно подробнее про товар?» и т.д. Когда владелец отвечает, что объявление давно снято или товар уже продан, мошенники не исчезают, а продолжают диалог. Они присылают ссылку на «то же самое объявление», которое якобы «до сих пор активно» и «висит на сайте».

Перейдя по ссылке, человек попадает на высококачественный клон официального сайта доски объявлений. Сайт выглядит абсолютно идентично оригиналу. Там просят:

Войти в свой аккаунт (логин и пароль);

Подтвердить данные через SMS-код;

Иногда сразу предлагают «обновить объявление» или «проверить статус».

Как только жертва вводит учётные данные, мошенники получают доступ к аккаунту. Дальше они могут:

Размещать от имени жертвы мошеннические объявления;

Красть личные данные и историю переписок;

Проводить дальнейшие этапы обмана (выманивать деньги, использовать аккаунт для других схем).

Главная опасность схемы – она выглядит как совершенно обычный и безобидный разговор с потенциальным покупателем. Нет прямых угроз, срочности или подозрительных просьб на первых этапах. Человек сам переходит по ссылке из любопытства или желания разобраться.

Ключевые советы, чтобы не попадать в такую ситуацию:

Никогда не переходите по ссылкам, которые присылают «покупатели» в ответ на ваши старые объявления.

Проверяйте статус объявления только самостоятельно – заходите на сайт напрямую через браузер или приложение, а не по ссылкам из сообщений.

Рекомендация: Даже если диалог выглядит полностью реальным и вежливым – не поддавайтесь любопытству. Любые ссылки от незнакомых «покупателей» – это потенциальная ловушка. Лучше удалить старое объявление или игнорировать такие сообщения.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА С ПОМОЩЬЮ СТАРЫХ ОБЪЯВЛЕНИЙ

БУДЬТЕ БДИТЕЛЬНЫ!
ЗАЩИТИТЕ СЕБЯ И СВОИ ДАННЫЕ!

Мошенники мониторят доски объявлений (Kufar и другие) и находят старые, давно закрытые объявления о продаже товаров, услуг, автомобилей, недвижимости и т.д.



КАК РАБОТАЕТ СХЕМА?

1 Мошенники пишут вам как обычные заинтересованные покупатели.

Здравствуйте, объявление ещё актуально?

Можно подробнее про товар?



2 Когда вы отвечаете, что объявление давно снято или товар продан, мошенники не исчезают.

Понятно. Но оно до сих пор активно и висит на сайте. Вот ссылка:

kufar.by/xxxxxx

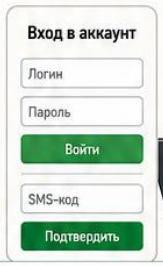


3 Вы переходите по ссылке и попадаете на высококачественный клон официального сайта доски объявлений.



4 На сайте просят:

- войти в аккаунт (логин и пароль);
- подтвердить данные через SMS-код;
- иногда сразу предлагают «обновить объявление» или «проверить статус».



5 Вы вводите данные – и мошенники получают доступ к вашему аккаунту.



6 Дальше они могут:

- Размещать от вашего имени мошеннические объявления
- Красть личные данные и историю переписок
- Проводить дальнейшие этапы обмана (выманивать деньги, использовать аккаунт для других схем)

Главная опасность схемы – она выглядит как совершенно обычный и безобидный разговор с потенциальным покупателем. Нет прямых угроз, срочности или подозрительных просьб на первых этапах. Человек сам переходит по ссылке из любопытства или желания разобраться.



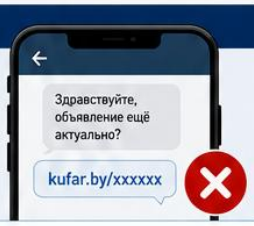
КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ:

1. НИКОГДА НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ,
которые присылают «покупатели» в ответ на ваши старые объявления.

2. ПРОВЕРЯЙТЕ СТАТУС ОБЪЯВЛЕНИЯ ТОЛЬКО САМОСТОЯТЕЛЬНО –
заходите на сайт напрямую через браузер или приложение, а не по ссылкам из сообщений.

РЕКОМЕНДАЦИЯ:

Даже если диалог выглядит полностью реальным и вежливым – не поддавайтесь любопытству. Любые ссылки от незнакомых «покупателей» – это потенциальная ловушка.
Лучше удалить старое объявление или игнорировать такие сообщения.



ПОМНИТЕ!
Ваша внимательность – лучшая защита от мошенников!
Проверяйте, прежде чем доверять.

102
Если вы стали жертвой мошенников – обращайтесь в милицию.

Распознавание и предотвращение мошеннических схем с «подарками от Ozon»

Мошенники массово рассылают фейковые электронные письма якобы от имени популярного маркетплейса Ozon. Письма оформлены очень качественно: используются официальные логотипы, фирменные цвета, шрифты и стиль компании.

В письме содержится поздравление: «Поздравляем! Вы выиграли приз в юбилейном розыгрыше Ozon!», «Ваш заказ стал победителем акции» или «Вы получили подарок на большую сумму». Указывается конкретный приз (смартфон, денежный сертификат, бытовая техника и т.д.) и заманчивая ссылка «Забрать приз», «Оформить доставку» или «Получить выигрыш».

Перейдя по ссылке, пользователь попадает на фишинговый сайт, который идеально копирует дизайн официального сайта Ozon. На сайте просят:

Войти в аккаунт (логин и пароль от Ozon);

Ввести данные банковской карты для «оплаты доставки», «таможенного сбора» или «подтверждения личности»;

Иногда просят код из SMS.

После ввода данных мошенники получают доступ к банковской карте и аккаунту Ozon. Деньги могут быть списаны мгновенно, а аккаунт использован для дальнейшего мошенничества (покупки на украденные средства, изменения данных и т.д.).

Схема особенно опасна в периоды крупных акций и юбилеев компании, когда люди действительно ожидают розыгрышей и подарков.

Ключевые советы, чтобы не попадать в такую ситуацию:

Не переходите по ссылкам из писем о выигрышах, подарках или розыгрышах, пришедших на почту.

Никогда не вводите данные карты или пароли на сайтах, к которым перешли по ссылке из письма. Ozon не сообщает о выигрышах через случайные email и не просит вводить данные таким образом.

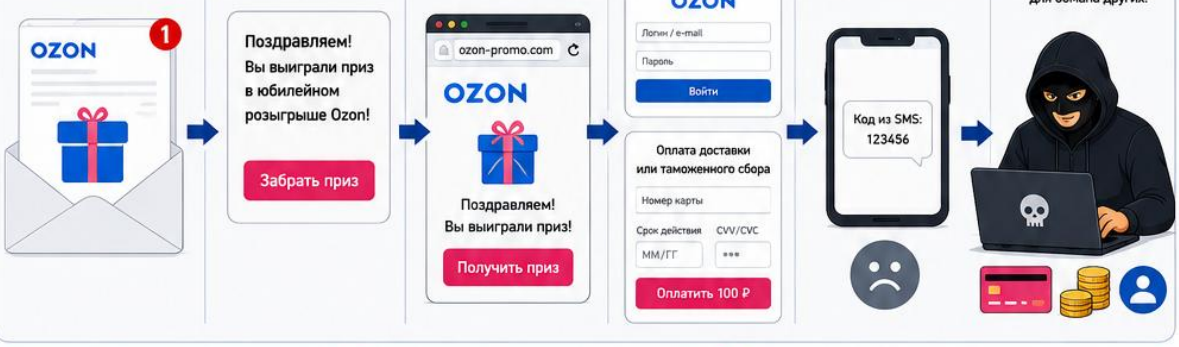
Рекомендация: Удаляйте такие письма. Акции и розыгрыши проверяйте только внутри официального приложения или на сайте Ozon.

ОСТОРОЖНО! МОШЕННИКИ РАЗДАЮТ «ПОДАРКИ ОТ OZON»

Мошенники рассылают фейковые письма от имени Ozon с сообщениями о выигрыше ценных призов.
Их цель – получить доступ к вашему аккаунту и банковской карте.

КАК РАБОТАЕТ СХЕМА

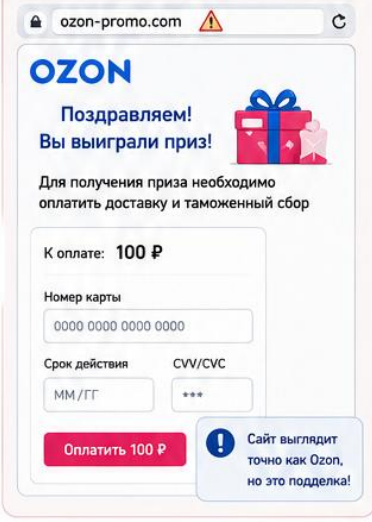
1. Вы получаете письмо на e-mail о выигрыше приза от Ozon.
2. В письме – поздравление, описание приза и кнопка-ссылка.
3. Вы переходите по ссылке и попадаете на поддельный сайт, похожий на Ozon.
4. Вас просят войти в аккаунт или ввести данные карты для получения приза.
5. Вы вводите данные карты или код из SMS.
6. Мошенники получают доступ к вашему аккаунту и карте. Деньги списываются, аккаунт – используется для обмана других.



ПРИМЕР ФЕЙКОВОГО ПИСЬМА



КАК ВЫГЛЯДИТ ФИШИНГОВЫЙ САЙТ



ЧЕМ ЭТО ОПАСНО?

- Кража денег с карты
- Доступ к вашему аккаунту Ozon
- Покупки на украденные средства
- Смена данных и управление аккаунтом
- Использование аккаунта для обмана других людей



Особенно активны мошенники во время крупных акций и юбилеев компании. Будьте бдительны!

КАК НЕ ПОПАСТЬСЯ НА УЛОВКУ МОШЕННИКОВ?

1. НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ ПИСЕМ

Не переходите по ссылкам из писем о выигрышах, подарках и розыгрышах, пришедших на почту.

2. НЕ ВВОДИТЕ ДАННЫЕ И ПАРОЛИ

Никогда не вводите данные карты, пароли и коды из SMS на сайтах, куда перешли по ссылке из письма.

3. ПРОВЕРЯЙТЕ ТОЛЬКО ОФИЦИАЛЬНЫЕ ИСТОЧНИКИ

Официальные розыгрыши и акции проверяйте только в приложении Ozon или на сайте ozon.ru.

РЕКОМЕНДАЦИЯ

- Удаляйте подозрительные письма, не переходите по ссылкам.
- Проверяйте информацию о акциях и розыгрышах только в официальном приложении или на сайте.
- Никому не сообщайте данные карты, пароли и коды из SMS!

БУДЬТЕ БДИТЕЛЬНЫ! ЗАЩИТИТЕ СЕБЯ И СВОИ ДЕНЬГИ!

Распознавание и предотвращение мошеннических схем с фейковыми уведомлениями от Apple

Мошенники массово рассылают фейковые уведомления через SMS, электронную почту, push-уведомления или сообщения в мессенджерах якобы от имени компании Apple.

В сообщении используется официальный стиль и дизайн: логотип Apple, фирменные шрифты и тревожный текст: «Внимание! В вашем хранилище iCloud заканчивается свободное место», «Если не обновить тариф в ближайшее время, все фотографии, видео, контакты и другие данные будут безвозвратно удалены». Часто добавляют счётчик дней («осталось 24 часа») для создания сильного чувства срочности.

В уведомлении содержится заманчивая кнопка или ссылка «Обновить хранилище», «Увеличить объём iCloud» или «Сохранить данные».

Перейдя по ссылке, пользователь попадает на высококачественный фишинговый сайт, который практически неотличим от официального сайта Apple (icloud.com или apple.com). На сайте просят:

Ввести данные Apple ID (логин и пароль);

Подтвердить вход кодом из SMS (двухфакторная аутентификация);

Иногда сразу предлагают привязать или подтвердить банковскую карту для «оплаты тарифа».

Как только жертва вводит данные, мошенники получают полный доступ к Apple ID. Это позволяет им:

Получить доступ ко всем фото, видео, переписке, документам и устройствам владельца;

Списывать деньги с привязанных банковских карт;

Использовать аккаунт для дальнейшего мошенничества (рассылка спама, запросы денег от имени жертвы и т.д.).

Схема очень эффективна, потому что многие пользователи iPhone действительно хранят важные данные в iCloud и боятся их потери.

Ключевые советы, чтобы не попадать в такую ситуацию:

Никогда не переходите по ссылкам из уведомлений об окончании места в iCloud или удалении данных.

Не вводите пароль Apple ID на подозрительных страницах. Проверяйте состояние iCloud только через официальные настройки iPhone.

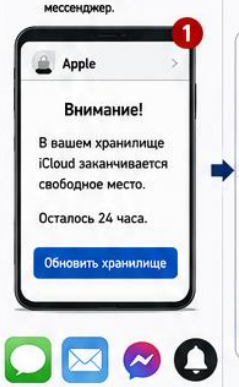
Рекомендация: При получении подобных уведомлений просто удалите их. Все важные действия с аккаунтом Apple выполняйте только внутри настроек устройства или на официальном сайте apple.com. Это поможет защитить ваши данные и аккаунт.

ОСТОРОЖНО! МОШЕННИКИ РАССЫЛАЮТ ФЕЙКОВЫЕ УВЕДОМЛЕНИЯ ОТ APPLE

Мошенники пугают потерей данных в iCloud, чтобы получить доступ к вашему Apple ID и украсть деньги.

КАК РАБОТАЕТ СХЕМА

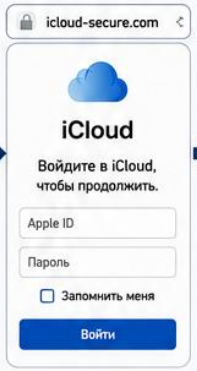
1. Вы получаете сообщение якобы от Apple через SMS, e-mail, push-уведомление или мессенджер.



2. В сообщении используют официальный стиль Apple и создают чувство срочности.



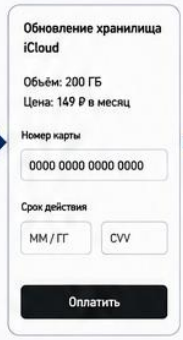
3. Вы переходите по ссылке и попадаете на фишинговый сайт, очень похожий на официальный.



4. Вас просят ввести данные Apple ID и подтвердить вход кодом из SMS.



5. Иногда сразу предлагают привязать или подтвердить банковскую карту для «оплаты тарифа».



6. Мошенники получают доступ к вашему Apple ID, данным, устройствам и банковским картам.



ЧЕМ ЭТО ОПАСНО?

ДОСТУП К ВАШИМ ДАННЫМ



Мошенники получают доступ ко всем фото, видео, контактам, переписке, заметкам, документам и резервным копиям iCloud.

СПИСАНИЕ ДЕНЕГ



Деньги списываются с привязанных банковских карт или оформляются платные подписки и услуги.

ИСПОЛЬЗОВАНИЕ АККАУНТА



Аккаунт используется для рассылки спама, обмана ваших контактов, запроса денег от вашего имени и других мошеннических действий.

ПОТЕРЯ УСТРОЙСТВ



Мошенники могут отслеживать ваши устройства, заблокировать их через режим пропажи или удалить данные.

СЛОЖНОСТИ ВОССТАНОВЛЕНИЯ



Восстановить доступ к Apple ID может быть очень сложно и долго, а данные могут быть безвозвратно потеряны.

КАК НЕ ПОПАСТЬСЯ НА УЛОВКУ МОШЕННИКОВ?

1 НИКОГДА НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ УВЕДОМЛЕНИЙ



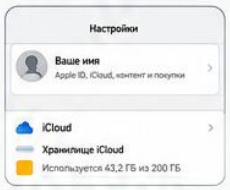
Apple не рассылает ссылки с просьбой обновить хранилище или подтвердить данные.

2 НЕ ВВОДИТЕ ПАРОЛЬ APPLE ID НА ПОДОЗРИТЕЛЬНЫХ САЙТАХ



Apple никогда не запрашивает логин, пароль или код из SMS через e-mail, SMS или push-уведомления.

3 ПРОВЕРЯЙТЕ СОСТОЯНИЕ ICLOUD ТОЛЬКО В НАСТРОЙКАХ IPHONE



Откройте «Настройки» → [Ваше имя] → iCloud → Хранилище iCloud.

4 ПРОВЕРЯЙТЕ АДРЕС САЙТА



Официальные сайты Apple: apple.com, icloud.com
Все остальные – подделки.

5 ОБРАЩАЙТЕ ВНИМАНИЕ НА ОШИБКИ И СРОЧНОСТЬ



Мошенники давят на страх, используют ошибки, странные адреса отправителей и грамматические неточности.

РЕКОМЕНДАЦИЯ

- ✓ Удаляйте подозрительные письма и сообщения.
- ✓ Все важные действия с Apple ID выполняйте только внутри настроек устройства или на официальном сайте apple.com.
- ✓ Включите двухфакторную аутентификацию для защиты аккаунта.
- ✓ Не сообщайте никому пароль и коды из SMS.

КАК ВКЛЮЧИТЬ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

1. Настройки → [Ваше имя] → Пароль и безопасность
2. Включите «Двухфакторная аутентификация»
3. Следуйте инструкциям на экране



ПОМНИТЕ: APPLE НИКОГДА НЕ ПРОСИТ ВВОДИТЬ ДАННЫЕ АККАУНТА ИЛИ КАРТЫ ЧЕРЕЗ ССЫЛКИ В ПИСЬМАХ И СООБЩЕНИЯХ!

БУДЬТЕ БДИТЕЛЬНЫ! ЗАЩИТИТЕ СВОЙ АККАУНТ И ДАННЫЕ!

Распознавание и предотвращение мошеннических схем с «подтверждением доставки»

Мошенники активно используют схему, связанную с доставкой товаров. Жертве звонит человек, представляющийся сотрудником службы доставки (СДЭК, Европочта, Яндекс.Доставка, Белпочта и др.). Он называет точный адрес, ФИО получателя и детали заказа. Всё звучит очень правдоподобно, особенно если человек действительно ожидает посылку (технику, телефон, одежду и т.д.).

Далее мошенник сообщает, что для передачи посылки нужно «подтвердить данные» или «пройти сверку», и присылает SMS-код. Он настойчиво просит назвать этот код по телефону. На уточняющие вопросы («почему нужен код?», «я могу подтвердить по-другому?») отвечает уклончиво или переводит разговор на другую тему, создавая ощущение срочности.

На самом деле полученный SMS-код используется для входа в банковские приложения, подтверждения операций, смены пароля в государственных сервисах или доступа к аккаунтам жертвы. В результате мошенники крадут деньги со счетов или получают доступ к личным данным.

Схема особенно опасна тем, что бьёт в момент наибольшего доверия – когда человек ждёт реальный заказ и меньше всего подозревает обман.

Ключевые советы, чтобы не попадать в такую ситуацию:

Никогда не называйте по телефону SMS-коды, пришедшие на ваш номер, даже если звонят якобы из службы доставки.

Помните: ни одна служба доставки не требует называть SMS-код для вручения посылки. Подтверждение доставки происходит лично при получении или через приложение/личный кабинет.

Рекомендация: Если вам звонят с просьбой назвать код из SMS – сразу прекращайте разговор. Перепроверьте статус заказа самостоятельно в официальном приложении или на сайте службы доставки. При любых подозрениях сообщайте в банк и в милицию.

РАСПОЗНАВАНИЕ И ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСКИХ СХЕМ С «ПОДТВЕРЖДЕНИЕМ ДОСТАВКИ»

СДЭК · ЕВРОПОЧТА · Яндекс Доставка · БЕЛПОЧТА

БУДЬТЕ БДИТЕЛЬНЫ – ВАШИ ДАННЫЕ ПОД ЗАЩИТОЙ!

Мошенники активно используют схему, связанную с доставкой товаров. Жертве звонит человек, представляющийся сотрудником службы доставки (СДЭК, Еропочта, Яндекс.Доставка, Белпочта и др.).

Он называет точный адрес, ФИО получателя и детали заказа. Всё звучит очень правдоподобно, особенно если человек действительно ожидает посылку (технику, телефон, одежду и т.д.).



КАК РАБОТАЕТ СХЕМА?

1. Мошенник звонит и представляется сотрудником службы доставки. Называет ваш адрес, ФИО и детали заказа. Всё выглядит очень достоверно.
2. Говорит, что для передачи посылки нужно «подтвердить данные» или «пройти сверку» и присылает SMS-код.
3. Настаивает назвать код по телефону. На вопросы отвечает уклончиво или создаёт ощущение срочности.
4. На самом деле код используется для входа в банковские приложения, подтверждения операций, смены пароля или доступа к аккаунтам.
5. Мошенники получают доступ к вашим счетам и личным данным и могут украсть деньги или использовать аккаунты в своих целях.



Схема особенно опасна тем, что бьёт в момент наибольшего доверия – когда человек ждёт реальный заказ и меньше всего подозревает обман.



КЛЮЧЕВЫЕ СОВЕТЫ, ЧТОБЫ НЕ ПОПАДАТЬ В ТАКУЮ СИТУАЦИЮ:



1. НИКОГДА НЕ НАЗЫВАЙТЕ ПО ТЕЛЕФОНУ SMS-КОДЫ, ПРИШЕДШИЕ НА ВАШ НОМЕР, даже если звонят якобы из службы доставки.



2. ПОМНИТЕ: НИ ОДНА СЛУЖБА ДОСТАВКИ НЕ ТРЕБУЕТ НАЗЫВАТЬ SMS-КОД ДЛЯ ВРУЧЕНИЯ ПОСЫЛКИ.

Подтверждение доставки происходит лично при получении или через приложение/личный кабинет.

РЕКОМЕНДАЦИЯ:

- Если вам звонят с просьбой назвать код из SMS – сразу прекращайте разговор.
- Перепроверьте статус заказа самостоятельно в официальном приложении или на сайте службы доставки.
- При любых подозрениях сообщайте в банк и в милицию.



Сообщите о мошенничестве: **102** в милицию

БУДЬТЕ БДИТЕЛЬНЫ!
ВАША ВНИМАТЕЛЬНОСТЬ – ЛУЧШАЯ ЗАЩИТА ОТ МОШЕННИКОВ!

НЕ ДАЙТЕ МОШЕННИКАМ ЗАВЛАДЕТЬ ВАШИМИ ДЕНЬГАМИ И ЛИЧНОЙ ИНФОРМАЦИЕЙ!