КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРМОШЕННИЧЕСТВА!

Кибермошенники постоянно совершенствуют методы обмана, используя новые технологии и социальную инженерию (методы манипуляции людьми). Ваша задача — быть в курсе актуальных схем мошенничеств и четко знать алгоритмы защиты.

1. Лжесотрудники госорганов и коммунальных служб

Суть схемы: Злоумышленники выдают себя за сотрудников коммунальных служб (Энергонадзор, Водоканал, Мингаз), банков, СК, МВД или КГБ. Они звонят по телефону (включая стационарные линии) или пишут в мессенджеры (Viber, Telegram, WhatsApp). Часто работают в паре: один сообщает о «утечке, раскрытии или изменения данных», второй (псевдосотрудник правоохранительных служб) требует оформить кредит или перевести деньги.

- **Уловка:** Требование срочно предоставить SMS-коды для «замены счетчиков» или авторизации, которые на самом деле открывают доступ к вашему профилю на порталах или интернет-банкингу.
- **Защита в Республике Беларусь:** Немедленно положите трубку. Помните: сотрудники ведомств Республики Беларусь никогда не звонят в мессенджерах по рабочим вопросам и не требуют перевода средств на «безопасные счета».

2. Мошенничество с использованием мобильной связи

Суть схемы: Мошенники представляются специалистами сотовых операторов Беларуси (A1, МТС, Life:) и заявляют, что срок действия вашей SIM-карты или договора истекает. Под предлогом продления услуг они присылают ссылку в мессенджере.

- **Уловка:** Ссылка ведет на скачивание вредоносного файла (.apk для Android). Установка такого приложения дает преступникам полный удаленный доступ к смартфону, включая чтение кодов из SMS, логинов и паролей к онлайн-банкингу.
- **Защита:** В Республики Беларусь договоры на мобильную связь являются бессрочными. Скачивайте приложения операторов исключительно из официальных магазинов (Google Play, App Store, App Gallery). Никогда не переходите по ссылкам от незнакомцев.

3. Использование дипфейков и нейросетей

Суть схемы: Киберпреступники взламывают аккаунт вашего родственника или знакомого и используют нейросети для генерации фальшивых голосовых сообщений или видео (дипфейков).

- **Уловка:** От имени близкого человека рассылаются сообщения с реалистичным голосом и просьбой срочно перевести деньги на лечение, после ДТП или перечислить средства через «общего знакомого».
- **Защита:** Свяжитесь с человеком по альтернативному каналу (обычный сотовый звонок, другая соцсеть). Задайте личный контрольный вопрос, ответ на который знает только ваш настоящий знакомый.

4. Психологическое давление и угрозы

Суть схемы: Аферисты представляются руководителями вашей организации или сотрудниками силовых ведомств (МВД, Следственный комитет, КГБ, ДФР, КГК).

- **Уловка:** Обвиняют в совершении преступления (например, в финансировании экстремизма или специальной военной операции на Украине) или соучастии в нем. Угрожают обысками, конфискацией имущества и тюремным сроком, требуя перевести сбережения на «защищенный счет» или передать наличные курьеру.
- **Защита:** Прервите разговор. Ни один руководитель или сотрудник силовых структур не ведет следственные действия через мессенджеры и не привлекает граждан к «секретным операциям» по переводу денег.

5. Финансовые пирамиды и лжеинвестиции

Суть схемы: Мошенники выступают в роли брокеров, трейдеров или экспертов криптобирж, гарантируя быстрый и аномально высокий доход.

- **Уловка:** Создаются фейковые сайты с графиками, имитирующими реальные торги, где жертве демонстрируют рост «прибыли». Для укрепления доверия могут разрешить вывести малую сумму. Цель — заставить внести крупные суммы, включая кредитные средства и деньги от продажи недвижимости.
- **Защита:** Инвестируйте только через организации, внесенные в официальные реестры Национального банка Республики Беларусь. Обещание гарантированной доходности — первый признак мошенничества.

6. Как не сделать iPhone «кирпичом» (Ловушки с Apple ID)

Механика обмана: Мошенники используют встроенную систему защиты Apple (функцию Find My / Локатор). Они заманивают жертву привлекательными предложениями легкого заработка или бесплатного контента, заставляя ввести чужой аккаунт Apple ID в настройки своего устройства.

- **Пример схемы «Заработок на играх/Тестировании»:** В Telegram или TikTok публикуются вакансии: «Требуется тестировщик мобильных игр. Задача — зайти под нашим корпоративным Apple ID, скачать новую игру (например, премиум-мод для PUBG или Standoff 2), проверить баги. Оплата 50 рублей в час».
- **Пример схемы «Помощь в чате»:** В игровых чатах или соцсетях новый «знакомый» пишет: «У меня сломался айфон, а там важные сохранения/контакты. Пожалуйста, зайди под моим iCloud со своего телефона на 5 минут, чтобы я мог сделать бэкап. Я заплачу».
- **Что происходит:** Как только вы вводите чужой Apple ID в основные настройки iPhone, злоумышленник удаленно включает через сайт icloud.com «Режим пропажи» (Lost Mode). Смартфон намертво блокируется (Activation Lock), а за пароль разблокировки требуют выкуп (от 300 рублей).

- **Правило защиты:** ***КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО*** вводить чужой Apple ID в настройки своего iPhone. Если вам необходимо использовать другой аккаунт для загрузки приложения, вводите его исключительно внутри магазина App Store. Никогда не платите шантажистам — после перевода денег они либо требуют еще, либо пропадают.
- **Что делать, если заблокировали:** Подготовьте коробку от устройства и официальный фискальный чек, подтверждающий покупку в белорусском магазине (A1, МТС, 5 элемент, iStore и др.). Обратитесь в официальную службу поддержки Apple через сайт — блокировку снимут бесплатно в течение нескольких дней после проверки документов.

7. Защита мессенджеров (Viber, WhatsApp, Telegram)

Схемы угона: Переход по ссылкам вида «Проголосуй за мою племянницу в конкурсе», «Получи бесплатную подписку Telegram Premium» или поддельные SMS о «необходимости верификации (проверки) аккаунта».

Меры жесткой защиты (Сделайте прямо сейчас):

- **Telegram:** Настройки → Конфиденциальность → Двухэтапная аутентификация. Установите облачный пароль и укажите email для восстановления.
- **Viber:** Настройки → Конфиденциальность → Двухфакторная проверка. Придумайте ПИН-код.
- **WhatsApp:** Настройки → Аккаунт → Двухшаговая проверка → Включить.
- **Контроль сессий:** Регулярно проверяйте раздел «Активные сеансы / Устройства» в настройках мессенджеров. При обнаружении незнакомых устройств немедленно нажимайте «Завершить все другие сеансы».

Алгоритм восстановления при взломе:

1. Зайдите в приложение и запросите код авторизации по SMS (или звонку). Если мошенники не успели установить свой облачный пароль, вы вернете доступ. Завершите все чужие сессии.

2. Если установлен чужой пароль, нажмите «Забыли пароль?». Восстановите доступ через ваш привязанный email.

3. Если мессенджер полностью заблокирован мошенниками, незамедлительно напишите в официальную службу поддержки (через сайты telegram.org/support, support.viber.com, whatsapp.com/contact).

8. Как проверить, нет ли на вас скрытых кредитов или банковских платежных карт

Контекст: Мошенники, получившие доступ к вашему паспорту или аккаунту МСИ, могут дистанционно открыть счета в белорусских банках или оформить онлайн-микрозаймы.

Как проверить тайные кредиты (Кредитный регистр Нацбанка Республики Беларусь):

- **Официальный способ контроля** — онлайн-портал creditregister.by.
- Для входа авторизуйтесь через Межбанковскую систему идентификации (МСИ) с помощью личного номера паспорта.

- Согласно законодательству Республики Беларусь, гражданин имеет право получить свой кредитный отчет 2 раза в календарный год совершенно бесплатно. В отчете будут видны все активные и закрытые кредиты, рассрочки, овердрафты во всех банках страны, а также список организаций, которые запрашивали вашу историю.

Как проверить открытые левые счета и карты (Система ЕРИП):

- В Республики Беларусь действует Межбанковская система идентификации (МСИ), оператором которой является ЕРИП.
- Зайдите в личный кабинет МСИ на сайте raschet.by или через авторизацию ЕРИП. В своем профиле вы можете увидеть, какие коммерческие банки имеют доступ к вашим актуальным данным. Если вы видите в списке банк, клиентом которого никогда не являлись — это повод для тревоги.
- Для полной проверки открытых счетов вы также можете обратиться в налоговые органы (Личный кабинет плательщика на portal.nalog.gov.by через вход по МСИ). В разделе данных о счетах отображаются все открытые на ваше имя счета в банках Республики Беларусь.
- При обнаружении несанкционированной карты или кредита немедленно свяжитесь с банком-эмитентом для блокировки счета.

9. Экстренная связь с крупнейшими банками Беларуси

Если вы передали данные карты мошенникам или подозреваете взлом, немедленно свяжитесь с банком для блокировки счетов по официальным коротким номерам:

Банк	Короткий номер	Тип связи / Особенности
Беларусбанк	**147**	Единый номер поддержки
Белагропромбанк	**136**	Единая инфолиния
Приорбанк	**487 / 729-90-90**	Для мобильных операторов
Сбер Банк (БПС)	**148**	Единый номер
Альфа-Банк	**7464**	Выделенный короткий номер
Банк ВТБ (Беларусь)	**250**	Для мобильных и городских звонков
Белинвестбанк	**146**	Контакт-центр
Белгазпромбанк	**120**	Единая служба поддержки

ПАМЯТКА ДЛЯ ГРАЖДАН РЕСПУБЛИКИ БЕЛАРУСЬ — СОХРАНИТЕ И ПЕРЕДАЙТЕ БЛИЗКИМ!

ОВД Гродненского райисполкома

КАК ОТСЕЧЬ ЗВОНКИ МОШЕННИКОВ: ПРОСТАЯ ИНСТРУКЦИЯ

Защитите себя, настроив популярные мессенджеры так, чтобы звонить вам могли ТОЛЬКО люди из вашей телефонной книги. Это займет меньше минуты!

В Viber:

Откройте Viber →
вкладка «Ещё» (внизу справа)→
Настройки →
Вызовы и сообщения.
Включите опцию ☑ «Защита от лишних звонков».

В Telegram:

Откройте Telegram → «Настройки» (шестеренка в меню) → Конфиденциальность → Звонки →
«Кто может звонить мне?».
Выберите вариант «Контакты».

В WhatsApp:

Откройте WhatsApp → вкладка «⋮» (три точки, Android) или «Настройки» (iOS) → Конфиденциальность → Вызовы.
Активируйте опцию «Тихие вызовы от неизвестных».

Помните:

1. Официальные структуры НИКОГДА не запрашивают по телефону коды из СМС, CVV-коды карт, пароли от интернет-банка или предложат установить посторонние программы.
2. Банки НЕ БЛОКИРУЮТ карты, предварительно не уведомив клиента через официальное приложение банка или СМС на короткий номер банка (который всегда одинаков и указан на обороте карты).
3. Любой звонок о проблемах с родственником ТРЕБУЕТ ПЕРЕПРОВЕРКИ. Немедленно положите трубку и самостоятельно позвоните родным или их близким знакомым по известным вам номерам.

Если вы пострадали от мошенничества:

1. Немедленно позвоните в свой банк по официальному номеру (с сайта или оборота карты), чтобы заблокировать карту (если сообщали реквизиты или коды).
2. Позвоните в межбанковскую систему идентификации по короткому номеру – 141! (заблокируют переводы ваших денежных средств).
3. Немедленно сообщите о происшествии в милицию по телефону 102! Чем быстрее вы обратитесь, тем выше шансы задержать преступников.

ОВД Гродненского райисполкома

🌲 Миллионы в дупле: как телефонные аферисты заставили пенсионерку из Скиделя спрятать валюту в лесу

Следственный комитет и милиция ОВД Гродненского райисполкома разбираются в обстоятельствах дерзкого и циничного мошенничества. Всего за один день жительница города Скидель лишилась суммы, эквивалентной почти 27 600 белорусских рублей. Поддавшись на уговоры «международных кураторов», женщина собственноручно отнесла тысячи долларов и евро в лесной тайник.

Преступление было совершено 17 июля. С 11 часов утра до половины десятого вечера потерпевшей буквально «обрывали» телефоны. Звонки поступали в мессенджерах Viber и Telegram.
Аферисты действовали организованно и использовали технологию подмены номеров. Женщине звонили якобы с белорусских номеров, а также с номеров иностранных операторов.

Преступники действовали под предлогом «необходимости декларирования денежных средств». Используя психологическое давление и манипуляции, они убедили жертву, что ее сбережения находятся под угрозой, и их нужно срочно передать для «проверки» или «легализации».

Под диктовку телефонных кураторов испуганная женщина собрала все свои накопления: **8 400 долларов США и 1 000 евро**.

Вместо того чтобы отправить жертву в банк, мошенники разыграли сценарий с тайником. Потерпевшая направилась в близлежащий лесной массив, там она нашла приметное дерево и **оставила пакет с валютой**. Естественно, как только женщина ушла, деньги забрал курьер.

Следователи и сотрудники милиции ОВД Гродненского райисполкома установили, что «кураторы» преступной схемы и организаторы звонков находились за пределами Республики Беларусь. Ущерб составил около 27 600 рублей, что по белорусскому законодательству признается **крупным размером**. По факту мошенничества возбуждено уголовное дело по ч.3 ст. 209 УК Республики Беларусь.

«Данный случай поражает своей циничностью, но, к сожалению, наглядно демонстрирует, насколько изобретательными становятся международные преступные группы. Мошенники используют глубокое психологическое давление, лишая людей способности мыслить критически.

Мы в очередной раз заявляем: **допущение подобных фактов — это результат излишней доверчивости и пренебрежения базовыми правилами цифровой и финансовой безопасности.**

Граждане должны четко усвоить: ни один официальный орган — будь то милиция, КГК, налоговая инспекция или банк — никогда не

решает вопросы декларирования, проверок или спасения расчетных счетов по телефону или в мессенджерах. И уж тем более государственные процедуры не проводятся через "тайники" в лесных массивах или дуплах деревьев. Любое требование перевести, спрятать или передать деньги незнакомцам — это стопроцентное преступление.

Наша общая задача — полностью исключить условия для таких преступлений. Профилактика должна дойти до каждого дома, до каждого пожилого человека. Если вам поступил подобный звонок — немедленно положите трубку и наберите 102. Этим вы защитите свои деньги и поможете нам задержать преступников».

ОВД Гродненского райисполкома

От «лишнего интернет-трафика» до «уголовного дела»: как международные аферисты запугали ребенка в Коробчицах и забрали золото на 20 тысяч рублей

Правоохранители Гродненщины раскрыли циничное преступление, в котором жертвой манипуляций стала несовершеннолетняя девочка. Всего за два дня — 8 и 9 августа — международные аферисты разыграли многоходовку, лишив семью крупных сбережений. За деньгами и драгоценностями в деревню Коробчицы приехала курьер — жительница одной из областей Беларуси.

Пошаговая схема: как ломали детскую психику

Следователи восстановили хронологию психологического давления на ребенка. Мошенники действовали по четко выверенному сценарию, меняя роли.

- **Шаг 1. Наживка с «интернет-трафиком».** Сначала девочке позвонил неизвестный. Он представился сотрудником компании МТС. Собеседник предложил заманчивую услугу — бесплатно увеличить лимит мобильного интернет-трафика. Доверчивый ребенок согласился и продиктовал пришедший на телефон СМС-код. Этот код открыл преступникам доступ к личным данным.
- **Шаг 2. Подключение «тяжелой артиллерии».** Сразу после этого в мессенджере раздался новый звонок. На этот раз звонивший представился сотрудником КГБ. Он огорошил ребенка заявлением: *«На твое имя прямо сейчас открыт подставной банковский счет, через который финансируются преступники»*.
- **Шаг 3. Запугивание и требование ценностей.** Пользуясь тем, что несовершеннолетняя не обладает жизненным опытом и испугалась «проблем с законом», лжесиловик потребовал срочно передать все имеющиеся дома ценности для «проверки и спасения семьи».

Финал в Коробчицах: визит курьера

Запуганная девочка, находясь под полным контролем кураторов, собрала семейные накопления. Для фиксации прибыли международные организаторы отправили на адрес в деревню Коробчицы своего курьера.

Приехавшая женщина (жительница одной из областей республики) забрала у ребенка:

- **600 долларов США** (1 758 белорусских рублей по курсу НБРБ).
- **Золотые изделия на сумму не менее 20 200 рублей**.

Общий имущественный вред превысил **21 958 рублей**.

Благодаря слаженным действиям сотрудников милиции ОВД Гродненского райисполкома, пособница зарубежных аферистов была оперативно установлена и задержана. Возбуждено уголовное дело за мошенничество в крупном размере по ч. 3 ст. 209 УК Республики Беларусь.

Комментарий руководства ОВД Гродненского райисполкома:

«Данная преступная схема наглядно показывает, насколько циничны международные аферисты. Они начали с банального предлога об интернет-трафике, а закончили жестким психологическим прессингом от имени

силовых ведомств. Ребенок просто не смог противостоять подготовленным манипуляторам.

Мы в очередной раз предупреждаем: допущение таких фактов — это повод для серьезного разговора внутри каждой семьи. Родители должны объяснить детям, что никакие вопросы с мобильными операторами или правоохранительными органами не решаются через СМС-коды втайне от взрослых.

Отдельно подчеркну: курьеры, приезжающие за деньгами, являются полноценными соучастниками. Жительница республики, забравшая золото в Коробчицах, действовала в составе группы с единым умыслом. Никакие оправдания о "простой подработке" не освобождают от уголовной ответственности и обязанности полностью возместить ущерб потерпевшим».

ОВД Гродненского райисполкома

Житель Гродненского района доверился «сотрудникам КГБ» и лишился более 79 тысяч рублей

Крупный случай телефонного и интернет-мошенничества зафиксирован в Гродненском районе. Житель агрогородка Озеры стал жертвой многоступенчатой преступной схемы, в которой злоумышленники представлялись налоговыми инспекторами, специалистами Национального банка и сотрудниками Комитета государственной безопасности. В результате обмана мужчина лишился 79 600 белорусских рублей, оформив крупные кредиты и продав собственный автомобиль.

Хронология обмана: от звонка в мессенджере до криптобиржи

История началась в конце июля 2026 года, когда потерпевшему в мессенджере «Viber» поступил звонок с неизвестного зарубежного номера. Звонивший представился сотрудником налоговой инспекции и под предлогом получения важного письма выманил у мужчины код из СМС-сообщения.

Сразу после этого к разговору подключились якобы представители Министерства связи, которые заявили, что личные данные гражданина похищены мошенниками. Чтобы «спасти» сбережения и предотвратить оформление фиктивных займов, мужчину убедили строго следовать инструкциям «специалистов».

Общение оперативно перевели в «Telegram», где с пострадавшим взаимодействовали фейковые аккаунты:

- Специальный бот, имитирующий структуру Национального банка Республики Беларусь;
- Псевдо-сотрудник Нацбанка;
- Лже-сотрудник следственного отдела КГБ.

По указке кураторов сельчанин начал «опережать мошенников» и брать реальные кредиты в различных банках страны. В общей сложности он оформил займы в пяти крупных банковских учреждениях на сумму более 57 тысяч рублей. Кроме того, поддавшись давлению, мужчина продал собственный автомобиль за 22 000 рублей, а вырученные деньги также пустил в оборот по указке преступников.

Все аккумулированные средства пострадавший переводил на специально открытый счет, после чего по инструкции «курирующих органов» зарегистрировался на криптовалютной бирже. Там белорусские рубли конвертировались в цифровую валюту (USDT) и отправлялись на указанный мошенниками криптокошелек.

Сейчас по факту хищения денежных средств проводится проверка. Сотрудники милиции проводят комплекс оперативно-розыскных мероприятий, направленных на установление лиц, причастных к преступлению.

Случай в аг. Озёры — не просто частная трагедия, а важное предупреждение для всех. Мошенники становятся всё изощрённее, но их схемы строятся на одних и тех же уязвимостях: спешке, страхе и доверии к «официальному тону». Главное оружие против них — пауза, проверка фактов и разговор с близкими перед любым финансовым решением.

ОВД Гродненского райисполкома

Осторожно: мошенники! Как жительница Гродненского района лишилась семейных сбережений после звонка от «Белпочты»

ОВД Гродненского райисполкома в очередной раз призывает граждан к бдительности. Мошенники продолжают использовать сложные многоступенчатые схемы психологического давления, вовлекая в свои сценарии фальшивых сотрудников государственных структур и правоохранительных органов.

В оперативно-дежурную службу ОВД Гродненского райисполкома обратилась жительница Гродненского района с заявлением о хищении крупной суммы денежных средств. Заявительница подробно описала механизм, с помощью которого злоумышленники завладели её семейными сбережениями.

Шаг 1. Звонок от имени «Белпочты»

Схема началась 14 сентября 2026 года с телефонного звонка в мессенджере Viber. Злоумышленник представился сотрудником РУП «Белпочта» и сообщил женщине ложную информацию о том, что на её адрес заказаны цветы. В ходе разговора потерпевшая подтвердила свои анкетные данные и сообщила, что находится на работе.

Для «подтверждения получения посылки» звонивший попросил продиктовать СМС-код, поступивший на её мобильный телефон. Как только жительница района передала код, доступ к её личным данным перешел в руки киберпреступников.

Шаг 2. Подключение «сотрудника правоохранительных органов» и «юриста Нацбанка»

Сразу после этого в диалог в мессенджере вступил якобы сотрудник кибербезопасности правоохранительных органов. Он применил тактику запугивания: сообщил, что под банковскими данными женщины осуществлен перевод **10 000 белорусских рублей** на имя лица, находящегося в межгосударственном розыске за измену Родине и терроризм. Гражданке пригрозили уголовной ответственностью за пособничество и реальным лишением свободы.

Для «урегулирования вопроса» потерпевшую перенаправили на подставного «юриста Национального банка Республики Беларусь». Чтобы окончательно подавить волю жертвы, мошенники продиктовали ей вымышленный номер уголовного дела и убедили перейти для дальнейшего общения в мессенджер Telegram.

Шаг 3. Дорогостоящее такси до Минска и «инкассаторы»

На следующий день, в схему включили лжесотрудника КГБ, который потребовал «сотрудничества ради избежание ответственности». Юрист Нацбанка дала указание собрать все находящиеся дома наличные деньги, сфотографировать их «стопками и веером» и отправить снимки обратно для «экспертизы по номерам купюр».

Потерпевшая упаковала все семейные сбережения — **650 евро, 1579 долларов США и 10 200 белорусских рублей** — в пакет, который обмотала

газетой и скотчем. По указанию кураторов из мессенджера жительница Гродненского района совершила следующие действия:

- Из отложенных денег оплатила такси для поездки в столицу.
- На вокзале пересела в другое такси, вызванное для неё мошенниками, и направилась в деревню Осово Минского района.
- Выйдя на остановочном пункте общественного транспорта «ВОСАВА», по указанию «юриста» она оставила пакет со всеми деньгами в условном скрытом месте якобы для «бесконтактной передачи инкассаторам»
- После этого потерпевшая вернулась обратно домой.

Финал преступной схемы

16 сентября мошенники прислали сообщение, что деньги «успешно получены инкассаторами» и проходят 3-дневную экспертизу. В течение последующих дней лжеэксперты Нацбанка переносили сроки созвона под предлогом занятости. На следующий день женщина обнаружила, что вся переписка в Viber удалена злоумышленниками. Осознав обман, гражданка незамедлительно обратилась в милицию. Примечательно, что женщина знала о подобных методах обмана из профилактических бесед, но в стрессовой ситуации поддалась жесткому психологическому давлению.

Комментарий руководства ОВД Гродненского райисполкома

Первый заместитель начальника ОВД Гродненского райисполкома подполковник милиции Барейша Евгений Степанович отмечает:

«Данный факт наглядно демонстрирует, насколько изощренными становятся методы современных киберпреступников. Они больше не ограничиваются банальными звонками от имени банковских служащих, а выстраивают целые цепочки, где жертве последовательно звонят "представители почты", "офицеры безопасности", "юристы Национального банка" и даже "сотрудники спецслужб".

Расчет мошенников всегда строится на факторе внезапности, дефиците времени и искусственном создании стрессовой ситуации — обвинении в финансировании терроризма. Под таким жестким психологическим давлением человек теряет способность к критическому мышлению. Переломным моментом здесь стала передача СМС-кода якобы для получения посылки, что открыло преступникам доступ к персональным данным.

Напоминаю каждому жителю района: ни одна государственная структура, будь то милиция, КГБ, Нацбанк или почтовая служба, не решает рабочие вопросы по телефону в мессенджерах. Мы не требуем проведения скрытых "операций", не просим фотографировать ваши сбережения и тем более не отправляем граждан на такси в другие регионы для передачи денег через тайники. Если вам поступил подобный звонок — немедленно положите трубку и сообщите в милицию по телефону 102. Помните, что сохранность ваших средств зависит в первую очередь от вашей бдительности».

ОВД Гродненского райисполкома

Новая уловка аферистов в Гродненском районе: как «запись к врачу» оборачивается потерей денег и взломом телефонов.

Правоохранительные органы Гродненского района бьют тревогу: в регионе участились случаи обращения граждан, ставших жертвами новой изощренной схемы киберпреступников. Мошенники сменили легенду и теперь маскируются под медицинских работников. Цель первого удара — выудить заветный СМС-код, после чего в дело вступает лжемиллиция.

Этап №1: Заботливый «медицинский работник»

Схема начинается с сообщения или звонка в мессенджере (Viber, Telegram, WhatsApp). Собеседник представляется сотрудником местной поликлиники или регистратуры.

Легенда обмана: Гражданину сообщают, что ему необходимо срочно пройти диспансеризацию, продлить флюорографию или заполнить «электронную медицинскую карту». Для подтверждения записи или верификации данных «медработник» просит назвать цифры, которые прямо сейчас пришли человеку в СМС-сообщении.

На самом деле этот код — ключ для доступа к личному кабинету пользователя в интернет-банкинге или для активации его мессенджера (Viber, Telegram, WhatsApp) на другом устройстве.

Этап №2: «Тяжелая артиллерия» от лжесиловиков

Как только испуганный или доверчивый гражданин диктует код, разговор прерывается, но тут же раздается новый звонок. На этот раз на связи «сотрудник правоохранительных органов» (МВД, Следственный комитет, КГБ).

Сценарий запугивания развивается по двум направлениям:

1. **Потеря контроля:** У человека мгновенно пропадает доступ к его собственной учетной записи в мессенджере. Преступники блокируют реального владельца и начинают от его имени просить деньги в долг у всех контактов в телефонной книге.
2. **Финансовый шантаж:** Лжесиловик строгим голосом сообщает: *«Вы только что передали секретный код мошенникам! Прямо сейчас от вашего имени открыт подставной банковский счет, через который финансируются преступники. Чтобы избежать обысков и уголовной ответственности, вам нужно действовать по нашей инструкции...»*. Далее жертву вынуждают переводить все личные сбережения на «безопасный счет» или оформлять огромные кредиты.

⚠ **Важно: Памятка безопасности для жителей района**

- **СМС-код — это личная цифровая подпись:** Его нельзя называть ни врачам, ни почтальонам, ни сотрудникам банков.
- **Перезвоните в регистратуру сами:** Если вам говорят о медкартах, повесьте трубку, найдите официальный номер своей поликлиники и уточните информацию.
- **Мессенджеры под защитой:** Обязательно установите в настройках Telegram и Viber **двухфакторную аутентификацию** (облачный пароль). Это не позволит мошенникам угнать ваш аккаунт, даже если они узнают СМС-код.

ОВД Гродненского райисполкома