белагропромбанк

МОШЕННИЧЕСКИЕ ОПЕРАЦИИ

с банковскими платёжными карточками

Распространенные схемы обмана

Правила безопасного использования карточки

Мошенники атакуют

топ – 6 схем обмана

1. Замена чипа к домофону
2. Фишинговые сайты
3. Легкий заработок
4. Ложный босс
5. Опасные приложения
6. Фейковый магазин

Топ – 6 схем обмана

Замена чипа к домофону 1

Как это работает

Мошенники звонят и сообщают, что в доме планируется замена домофонов и чипов к ним.

Уточняют ФИО и иные персональные данные.

Направляют СМС с кодом, который нужно сообщить для «регистрации» в системе.

Далее звонит «милиционер»: - «На ваше имя оформлен кредит и средства переведены в недружественные страны.

Вам грозит обыск и изъятие всех денежных средств – срочно нужно перевести все сбережения на «специальный безопасный» банковский счёт»

Мошенники могут представляться также:

- сотрудниками налоговой службы для уплаты пени по налогам;
- работниками поликлиники для прохождения диспансеризации;
- работниками Белпочты для получения заказного письма/посылки;
- работниками Энергосбыта или Водоканала для замены счетчиков.

Правило безопасности

Незамедлительно прервать телефонный разговор.

Ни при каких обстоятельствах не сообщать личных данных, кодов из СМС, данных платёжной карточки, паролей и логинов к банковским приложениям.

Ни одна официальная организация не будет запрашивать паспортные данные или коды из СМС-сообщений по телефону через мессенджер.

Фишинговые сайты 2

Легкий заработок 3

Ложный босс 4

Опасные приложения 5

Фейковый магазин 6

Топ – 6 схем обмана

2 Фишинговые сайты
(опросы и реклама в сети)

Как это работает

Вам предлагают участие в «розыгрыше призов».

Для этого нужно перейти по ссылке и авторизоваться.

Ссылка ведёт на поддельный сайт с мошенническим доменом.

Дизайн мошеннического сайта выглядит как ресурс банка, но это подделка.

Цель мошенников — украсть ваши данные и СМС-коды.

Признаки фишинговой страницы

1. Адресная строка (URL) – главное слабое место.
2. Замочек и HTTPS – не гарантия, но важно

В адресной строке должен быть значок закрытого замка, а адрес — начинаться с https://.

3. Ошибки и «кривой» дизайн.
4. Подозрительные запросы данных.
5. Психологическое давление.

Правило безопасности

Если ссылка пришла от незнакомого контакта или в рекламе — **не переходите по ней.**

Лучше сами вбейте название сайта в поиске и зайдите через официальную страницу.

Лёгкий заработок 3

Ложный босс 4

Опасные приложения 5

Фейковый магазин 6

Замена чипа к домофону 1

Топ-6 схем обмана

Лёгкий заработок 3

Как это работает

Предлагают лёгкий заработок: «Нужны люди для приёма переводов на карточку и пересылки дальше, без вложений, платим процент», иногда маскируют под работу курьером или «финансовым помощником».

Что реально происходит

На карточку «посредника» приходят деньги, добытые мошенниками (украденные с чужих карточек, полученные по поддельным кредитам и т.п.).

Посредник снимает наличные или переводит их дальше по указанию «работодателя» и оставляет себе небольшой процент как «заработок».

Правило безопасности

Если вам предлагают лишь дать карточку/снять деньги, а источник денег непонятен – это почти всегда схема с чужими украденными деньгами.

Тот, кто «просто перевёл» или «просто снял» деньги, в глазах закона – не жертва, а участник преступления, даже если он не знал.

Ложный босс 4

Опасные приложения 5

Фейковый магазин 6

Замена чипа к домофону 1

Фишинговые сайты 2

Топ – 6 схем обмана

Ложный босс 4

Как это работает

Мошенники собирают сведения о работниках организации в чатах и каналах в мессенджерах, в соцсетях.

Далее злоумышленник регистрирует в мессенджере (чаще в Telegram) поддельный аккаунт на имя руководителя организации: в аккаунте указывают ФИО руководителя, добавляют его фотографию – всё это также получено из открытых источников сети Интернет.

Что происходит дальше

Этап 1. Подготовка
«Руководитель» вступает в переписку с работником на бытовые темы

Этап 2. Подключение «правоохранителя»
«Руководитель» сообщает о скором звонке от представителя надзорного органа

Этап 3. Вымогательство
«Правоохранитель» звонит работнику и требует:

- перевод денег на «защищённый счёт»;
- установку ПО для удалённого управления телефоном;
- фотографии банковских карт.

Правило безопасности

- не оставляйте информацию о рабочем электронном почтовом ящике в сети Интернет, а также без особой необходимости не указывайте сведения о месте вашей работы;
- не публикуйте фотографии служебного удостоверения, бейджа;
- не переводите деньги по просьбе третьих лиц (в т.ч. руководителя, полученной по мессенджеру).

Опасные приложения 5

Фейковый магазин 6

Замена чипа к домофону 1

Фишинговые сайты 2

Лёгкий заработок 3

Топ – 6 схем обмана

5 Опасные приложения

Как это работает

Злоумышленники под видом службы поддержки оператора связи (A1, МТС, Life) рассказывает легенду, что нужно продлить срок действия сим-карты.

Это могут быть «специалисты» отдела безопасности банка с предложением установить «приложение для защиты устройства от хакеров».

Присылают ссылку на скачивание приложения личным сообщением в мессенджере.

Что реально происходит

Как только приложение загружается на телефон, оно просит доступ к SMS и управлению телефоном.

Таким образом мошенники получают полный доступ ко всем данным, хранящимся на телефоне.

Правило безопасности

Никогда не скачивайте приложения по просьбе «операторов связи», «банка» или «службы безопасности».

Устанавливайте программы только через официальные магазины Google Play или App Store.

Запомните – банк сам защитит ваш счёт, никакие дополнительные приложения для этого не нужны.

6 Фейковый магазин

1 Замена чипа к домофону

2 Фишинговые сайты

3 Лёгкий заработок

4 Ложный босс

Топ – 6 схем обмана

Фейковый магазин 6

Как это работает

Мошенники максимально активизируются в период распродаж.

Они подделывают интернет-магазины, в том числе и в социальных сетях.

Их главная уловка – низкие цены, а товары обещают доставить быстро.

Признаки фейк-магазина

1. У магазина нет истории

Фейковые страницы запускаются под распродажи.

У них нет старых постов, живых отметок и комментариев.

2. Скрытые контакты

В описании профиля нет рабочего телефона и реального адреса.

Вам предлагают общаться только в личных сообщениях.

3. Цена и условие оплаты

Товар стоит на 70–90% дешевле рынка.

Цена создана, чтобы заставить вас действовать быстро, отключив бдительность.

Правило безопасности

Никогда не скачивайте приложения по просьбе «операторов связи», «банка» или «службы безопасности».

Устанавливайте программы только через официальные магазины Google Play или App Store.

Запомните – банк сам защитит ваш счёт, никакие дополнительные приложения для этого не нужны.

Замена чипа к домофону 1

Фишинговые сайты 2

Лёгкий заработок 3

Ложный босс 4

Опасные приложения 5

Что делать, если позвонили мошенники…

Прекратите разговор и положите трубку

Не паникуйте, расскажите о ситуации родным и близким, не молчите

Перезвоните в организацию по официальному номеру телефона для проверки информации

Не выполняйте никаких инструкций от неизвестных лиц

Что делать, если Вас обманули…

Срочно позвоните в банк по номеру 136 и заблокируйте карточку или сделайте это в мобильном приложении

Сохраните все SMS и скриншоты переписки с мошенниками

У Вас есть 30 дней, чтобы заявить о мошенничестве и краже

белагропромбанк

БЕРЕГИТЕ СВОИ ФИНАНСЫ!

ОАО «Белагропромбанк»

www.belapb.by

2026