Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

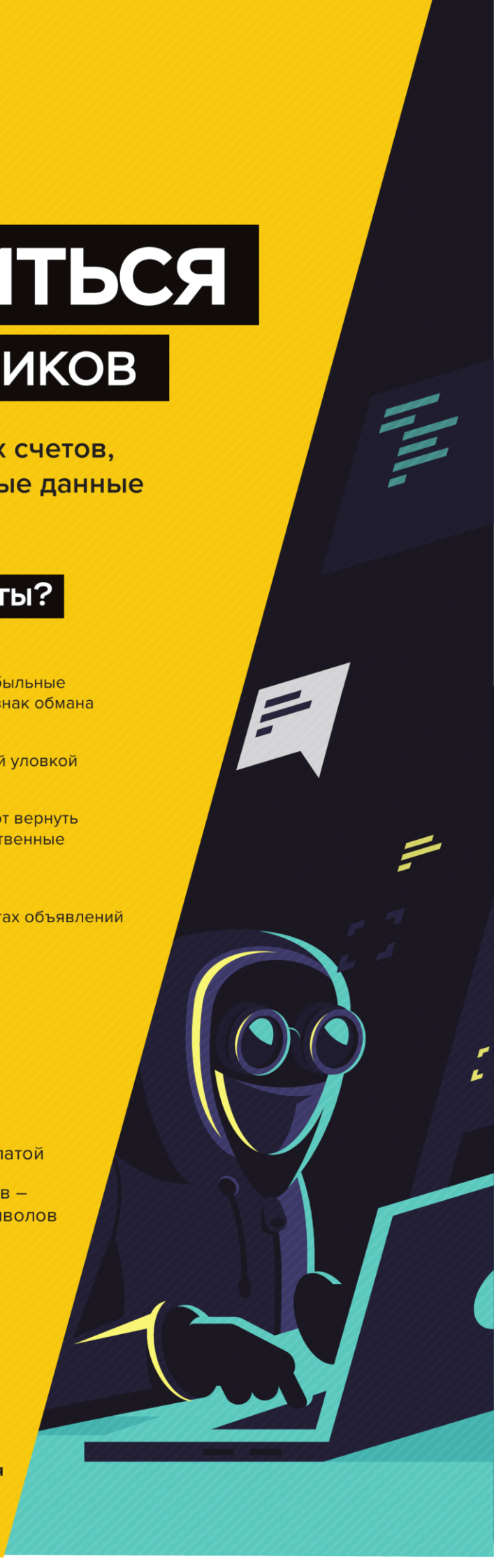
Как защитить свои финансы, читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт



Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ

- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ

Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура

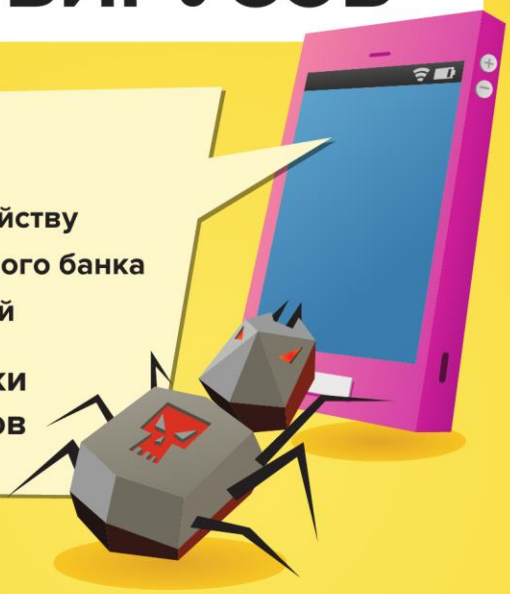
Банк России

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- **Обратитесь в сервисный центр**, чтобы вылечить гаджет
- **Перевыпустите карты, смените логин и пароль** от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- **Используйте антивирус** и регулярно его обновляйте
- **Не переходите по ссылкам** от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- **Обновляйте** операционную систему устройства
- **Избегайте** общедоступных Wi-Fi-сетей

Подробнее о защите гаджетов читайте на fincult.info

Финансовая культура

НЕ ДАЙ ОБМАНУТЬ СЕБЯ МОШЕННИКАМ!

1 МОШЕННИКИ ШЛЮТ «ПИСЬМА СЧАСТЬЯ» И ЖДУТ, КОГДА ВЫ ПОПОЛНИТЕ ИХ КОШЕЛЕК СВОИМИ ДЕНЬГАМИ!

НЕ ОТВЕЧАЙТЕ НА ТАКИЕ СМС!!!

- **КАРТА ЗАБЛОКИРОВАНА. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ**
- **ВЫ ВЫИГРАЛИ АВТОМОБИЛЬ! ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ**
- **ПОПОЛНЕНИЕ СЧЕТА НА 20 000 РУБЛЕЙ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ**
- **НАПОМИНАЕМ ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО КРЕДИТУ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ**
- **МАМА, У МЕНЯ ПРОБЛЕМЫ. ПОТОМ ВСЕ ОБЪЯСНЮ. ПЕРЕВЕДИ 300 РУБЛЕЙ НА ТЕЛ. ХХХХХ.**

2 У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

МОШЕННИКИ ПРЕДЛАГАЮТ ПО АКЦИИ УДВОИТЬ ПЕНСИЮ. ПОМОЧЬ ПОПАВШЕМУ В ДТП ВНУКУ, ВНЕ ОЧЕРЕДИ ПРОЙТИ МЕДИЦИНСКОЕ ОБСЛЕДОВАНИЕ.

НЕ ПЕРЕДАВАЙТЕ И НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НЕЗНАКОМЦАМ.
ПРОВЕРЬТЕ ПОСТУПИВШУЮ ИНФОРМАЦИЮ, ПОЗВОНИТЕ РОДСТВЕННИКАМ ИЛИ 02.

3 МОДНЫМ И НАИВНЫМ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯМ ПОСВЯЩАЕТСЯ!

В СОЦИАЛЬНЫХ СЕТЯХ, НА САЙТАХ «АВИТО», «ДРОМ.РУ» ДОВЕРЧИВЫМ ПОКУПАТЕЛЯМ ПРЕДЛАГАЮТ ВНЕСТИ ПРЕДОПЛАТУ ЗА НЕСУЩЕСТВУЮЩИЙ ТОВАР, ОДНАКО В ДАЛЬНЕЙШЕМ СВЯЗЬ С ЛЖЕПРОДАВЦАМИ ПРЕКРАЩАЕТСЯ.

4 РУЧКУ ПОЗОЛОТИ, ВСЮ ПРАВДУ РАССКАЖУ

МОШЕННИКИ ПРЕДЛАГАЮТ ЧУДОДЕЙСТВЕННОЕ ИСЦЕЛЕНИЕ ОТ ПОРЧИ ИЛИ СГЛАЗА.
ОДНАКО, ГЛАВНАЯ ИХ ЦЕЛЬ - ЗАВЛАДЕТЬ ВАШИМИ ДЕНЕЖНЫМИ СРЕДСТВАМИ, ЦЕННЫМИ ВЕЩАМИ И СКРЫТЬСЯ . **НЕ ВЕРЬТЕ «ЛЖЕЦЕЛИТЕЛЯМ» И ГАДАЛКАМ!!!**

ОСТОРОЖНО: МОШЕННИКИ!
НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Будьте бдительны при совершении действий с банковскими картами и соблюдайте элементарные правила безопасности, чтобы не стать жертвой мошеннических действий.

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Вам поступил звонок (сообщение) о блокировке банковской карты или подозрительных операциях с деньгами – это **МОШЕННИК**. Прекратите разговор и позвоните на горячую линию банка.

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Вам позвонили от имени близкого человека, сообщили о несчастном случае и требуют деньги – это **МОШЕННИК**. Прекратите разговор и позвоните близкому человеку.

СООБЩЕНИЕ В СОЦИАЛЬНОЙ СЕТИ

Ваш друг (родственник) пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные Вашей карты, чтобы перечислить их Вам, скорее всего - это **МОШЕННИК.**

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

По Вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты и смс-код, чтобы перевести деньги - это **МОШЕННИК.**
Прекратите разговор и ни в коем случае не сообщайте код.

Не доверяйте банковские карты третьим лицам, не оставляйте их без присмотра – так ими легко может воспользоваться МОШЕННИК.

В случае потери или хищения банковской карты немедленно обратитесь в банк.

В случае хищения Ваших денег или при подозрении совершения в отношении Вас мошеннических действий, немедленно позвоните в полицию.

Департамент безопасности жизнедеятельности Администрации города Тюмени

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«ВАША КАРТА ЗАБЛОКИРОВАНА»
SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»
Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»
SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»
Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»
просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Помните! Если вам звонят и тревожным голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники!
Никогда не проходите по ссылкам присланный в SMS-сообщении с незнакомых номеров!
Никому не сообщайте ПИН-код вашей банковской карты!

Звоните 02 или 102

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

КАК РАСПОЗНАТЬ ТЕЛЕФОННОГО МОШЕННИКА

ОМВД России «Няндомский» предупреждает!

ЕСЛИ ВАМ СООБЩИЛИ ПО ТЕЛЕФОНУ, ЧТО:

- ваша банковская карта заблокирована...
- необходимо пополнить баланс неизвестного номера телефона...
- нужны деньги, чтобы спасти попавшего в беду родственника
- вы выиграли приз...
- вам полагается компенсация...

ПОМНИТЕ: ЭТО ОРУДУЮТ ТЕЛЕФОННЫЕ МОШЕННИКИ!

Звони 02 или 102

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

АДМИНИСТРАЦИЯ ГОРОДА КИРОВ

УМВД РОССИИ ПО КИРОВСКОЙ ОБЛАСТИ

ОСТОРОЖНО, МОШЕННИКИ!

РЕКОМЕНДАЦИИ, КОТОРЫЕ ПОМОГУТ СОХРАНИТЬ ВАШИ ДЕНЬГИ И ЦЕННОСТИ

Вы получили СМС подозрительного содержания и адресата (с просьбой перевести деньги, подтвердить запрос, передать данные и т.д.)

Не торопитесь совершать ожидаемые от вас действия. В случае необходимости адресат свяжется с вами по телефону.

Вам звонят по телефону и сообщают якобы важную информацию (блокировка карты, беда с родственником, получение выигрыша и т. д.)

Проверьте полученную информацию из других источников (в банке, у родственника либо организации).

Вы натолкнулись на подозрительное сообщение/объявление в сети Интернет (просьба помочь от друга, продажа несуществующего товара либо его подделки, перевод денег на карту и т.д.)

Относитесь критично к навязываемым вам в сети Интернет предложениям. Перепроверяйте информацию. Прочтите отзывы, свяжитесь с продавцом, не переводите деньги и не направляйте информацию о своих банковских картах непроверенным источникам.

К вам пришли незнакомцы и предложили услуги (работники социальных и коммунальных служб, продавцы медицинских препаратов и т.д.)

Уточните по телефону в организации работает ли у них данный сотрудник, попросите предъявить удостоверение, не спешите соглашаться на предлагаемые услуги, попросите подойти позднее, посоветуйтесь с родственниками и специалистами.

При подозрении на совершение против вас мошеннических действий незамедлительно обратитесь в полицию.

02,102 (с мобильного)

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ПО ТЕЛЕФОНУ НЕЛЬЗЯ:

Выиграть миллион рублей!

Разблокировать банковскую карту!

Получить компенсацию от банка!

Приобрести редкие товары и уникальные таблетки!

Спасти близкого человека, попавшего в беду!

ДЛЯ ПЕРЕВОДА ДЕНЕГ ДОСТАТОЧНО ЗНАТЬ ТОЛЬКО НОМЕР КАРТЫ ИЛИ МОБ.ТЕЛЕФОН ЕЕ ВЛАДЕЛЬЦА. ИНЫЕ СВЕДЕНИЯ ДАДУТ ПРЕСТУПНИКУ ВОЗМОЖНОСТЬ РАСПОРЯДИТЬСЯ ВАШИМИ СБЕРЕЖЕНИЯМИ ДИСТАНЦИОННО.

ПО ТЕЛЕФОНУ МОЖНО:

СТАТЬ ЖЕРТВОЙ МОШЕННИКА!

ПРИ НАЛИЧИИ СОМНИТЕЛЬНЫХ ПРЕДЛОЖЕНИЙ

ОБРАЩАЙТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНУ - 02 ИЛИ 102 (С МОБИЛЬНОГО)

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

Здравствуйте, Мария Ивановна!
Я работник службы безопасности банка.
С вашей карты совершается перевод.
Подтверждаете его?

ПОЛОЖИТЕ ТРУБКУ

ПОЛОЖИТЕ ТРУБКУ

Здравствуйте, Николай Петрович!
Я сотрудник вашего банка.
Ваша карта подверглась атаке.
Для сохранения средств переведите их на резервный счет.

ПОЛОЖИТЕ ТРУБКУ

Здравствуйте, я сотрудник финансового мониторинга банка.
По реквизитам вашей карты оформляется кредит.
Вы подтверждаете оформление кредита?