Популярная схема обмана

Фишинг по СМС

- Вы получаете СМС, например, о подключении услуги или о списании денег с вашего счета.
- Чтобы узнать подробности, вам предлагают перейти на мошеннический сайт и авторизоваться, используя логин и пароль от онлайн-банка.
- Если выполнить это требование, мошенники могут украсть ваши конфиденциальные данные и использовать их для получения доступа к вашему личному кабинету, а также заразить телефон вирусом.

Всегда найдутся люди, которые попытаются украсть ваши данные и незаконно получить ваши деньги.

Сотрудники банка никогда не запрашивают полный номер карты, пароли и коды.

Если у вас есть подозрение, что вас обманывают, сразу свяжитесь с банком одним из этих способов:

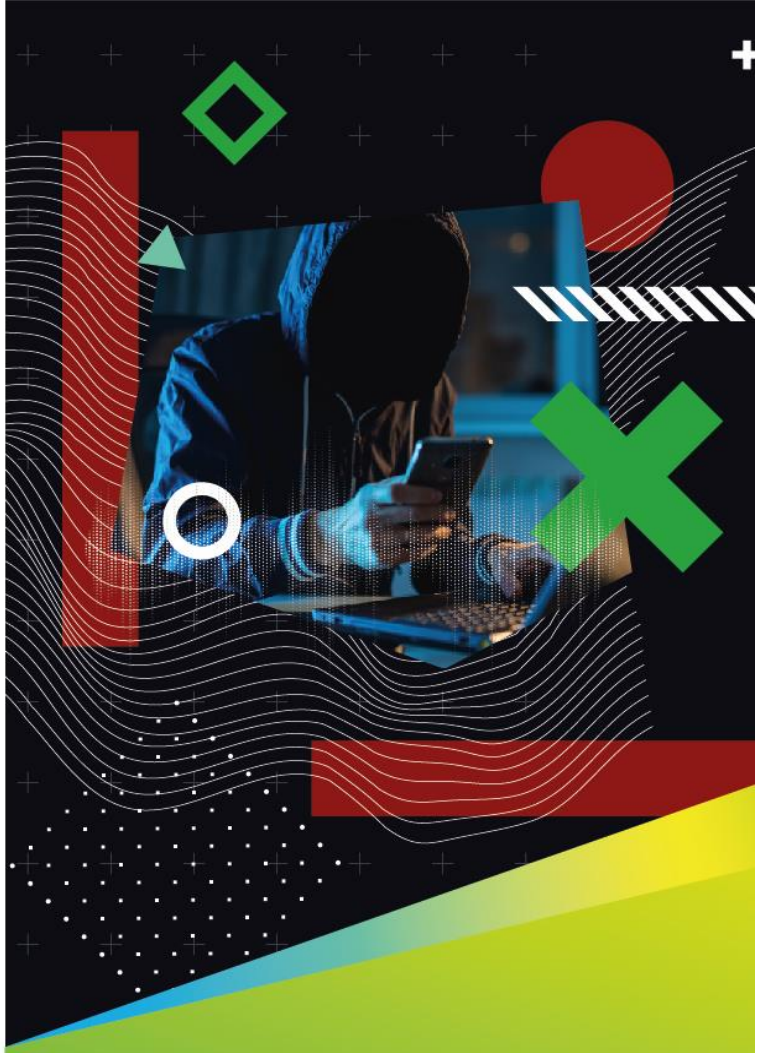
1. По номеру 5 148 148 (A1, МТС, life) или единому номеру 148.

2. В мобильном приложении Сбербанк Онлайн (иконка "Связь с Банком" в меню профиля слева).

Как защититься:

- Помнить, что отправителем сообщений от Сбер Банка отображается только SBER BANK.
- Прежде, чем переходить по ссылке, нужно убедиться, что она ведёт именно на сайт Сбер Банка, — мошенники используют внешне похожие домены.
- Настроить блокировку фальшивых сайтов в своём браузере.
- Не вводить данные, если домен несовпадает с официальным названием сайта.
- Приложение Сбербанк Онлайн необходимо устанавливать только из официальных магазинов (Google Play, Apple Store).
- Если вы перешли по подозрительной ссылке и ввели учётные данные, необходимо срочно сменить логин и пароль.

148 | 5 148 148 (A1, МТС, LIFE)



СБЕР БАНК

Как защитить себя от мошенников

sber-bank.by

Социальная инженерия – воздействие мошенников на людей, при котором люди сами отдают свои деньги или сообщают конфиденциальные данные.

Распространенные виды мошенничества

Фишинг

Когда мошенники «выуживают» личные данные – логины, пароли, коды из СМС – через СМС, письма и подменные сайты.

Мошенничество по телефону

Когда злоумышленники звонят вам или просят им позвонить и «выуживают» личные данные и под разными предлогами просят перевести деньги.

Что нужно мошенникам

Данные банковских карт: коды из СМС, номер карты, CVV/CVC-код (трехзначный код на оборотной стороне карты), логин и пароль от интернет-банка.

Чтобы вы перевели деньги на счет мошенника, например, для спасения средств, выгодной сделки или помощи попавшим в беду.

- Если у вас запрашивают эти данные по телефону, кладите трубку.
- Если данные запрашивают на сайте, то проверяйте название сайта, логин и пароль вводите только на официальном сайте банка.

ФЕЙК! www.sberdank.by — d вместо b

оригинальный сайт www.sber-bank.by

СХЕМЫ ОБМАНА

Звонок из «службы безопасности банка

Номер телефона обычно похож на банковский, (например, +375 29 914 81 48 вместо +375 29 514 81 48), а звонящий представляется сотрудником службы безопасности. Он говорит, что банк якобы выявил подозрительную операцию или в системе произошёл сбой.

Затем просит назвать полные данные карты, код безопасности на оборотной стороне карты, код из СМС или пароли от Сбербанк Онлайн, чтобы «защитить» ваши деньги. Для убедительности может сказать, что включает программу-робот, что только роботизированной системе можно сообщать данные. Кроме того, может предложить перевести деньги на «защищённый счёт» персонального менеджера.

Как защититься

- Не совершать никаких операций по инструкциям звонящего.
- Сразу закончить разговор, если кто-то просит у вас данные карты или интернет-банка.
- Если мошеннику удалось узнать у вас какую-то информацию, сразу позвонить в банк и сообщить о случившемся.

Звонок от «покупателя»

Если вы оставляли своё имя и номер телефона на сайте объявлений, мошенник может представиться покупателем.

Он попросит у вас для оплаты не только номер карты, но её CVV-/CVC-код или код из СМС.

Как защититься

- Помнить, что для перевода на вашу карту покупателю достаточно знать только её номер и срок действия или телефон, привязанный к ней.
- Не сообщать никому CVV-/CVC-код (трехзначный код на оборотной стороне карты), код из СМС, пароли от мобильного и интернет-банка.

Опрос от имени Сбер Банка

Вы видите рекламу в социальных сетях или получаете сообщение с предложением пройти опрос и **получить за это денежное вознаграждение**. После завершения опроса вас могут попросить перечислить «закрепительный платёж» для подтверждения карты и перечисления бонусов. Вы отправляете деньги, а потом не можете связаться с мошенниками.

Как защититься

- Помнить: Сбер Банк никогда не проводит опросы за вознаграждение.
- Настроить блокировку фальшивых сайтов в своём браузере.
- Не вводить данные, если домен не совпадает с официальным названием сайта (например, sberdank.by), а адрес сайта начинается с http, а не https