

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 ПОДАРОМ

Сильные эмоции притупляют бдительность.

3 ЗВОНЯТ

«Ваша карта заблокирована»

4 УВЕДИТЕСЬ

«или вы не являетесь клиентом»

5 НА ВАС ДАВЯТ

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

6 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти ситуацию, получить компенсацию или вложиться в инвестиционный проект.

7 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений.

ВАЖНО!

Сотрудники банка 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
- кодовые слова
- персональные данные

Как проверить свои банковские счета на fssb.ru

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?

ОФЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Специально созданные сайты, социальные выплаты или конкурсы призывают к участию. Там вас ждут денежные вознаграждения – призы, подарки.

ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Отправляют смс и письма, где говорится о возможности приобрести уникальные товары по сниженным ценам.

СПЕКУЛИРУЮТ НА ГРОМКИХ СООБЩЕНИЯХ
Написав, что вы выиграли крупную сумму, аферисты просят сообщить свои данные, чтобы вы могли получить выигрыш.

МАСКИРУЮТСЯ
Иногда аферисты, продавая и покупая на популярных сайтах, объявляют о своих услугах.

Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его.
- 2 Заведите отдельную дебетовую карту для покупок в интернете и используйте ее только для покупок.
- 3 Всегда проверяйте адрес электронной почты и сайта – вы можете столкнуться с фишингом, если перейдете по ссылке из ненадежного источника.
- 4 Не переходите по ссылкам из ненадежных источников.
- 5 Никогда не сообщайте свои персональные данные.

Как проверить свои банковские счета на fssb.ru

Финансовая культура

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 ссылке из интернета или электронной почты, СМС, сообщениям в соцсетях или мессенджерах, рекламе, объявлениям о розыске, распродажах, конкурсах, от государства.

Хакеры часто используют чужие аккаунты, и фишинговые сайты могут 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 выглядит некачественно, в тексте 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.

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 операциями



- Заявление должно быть написано:
- в течение суток после совершения в отделении банка
- 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:

- данные карты и пин-код, на ее обратной стороне (CVV/CVC)
- пароли и коды из уведомлений
- пароли и пароли от почты банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

напишите только сотруднику банка, когда сами позвоните на горячую линию.



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

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

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

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



КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАИЖИЖНО?

- Всплывает, перезагружается или отключается
- Сам замедляет работу приложений
- Показывает использование памяти
- Таргет объявляем

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- Позвоните в банк и попросите заблокировать доступ к почте и мобильному банку и все карты, которые использовались на устройстве
- Обратиться в сервисный центр, чтобы выключить гаджет
- Перезагрузите карты, смените логины и пароли от почты-банка и банка-установите банковские приложения

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- Используйте антивирус и регулярно его обновляйте
- Не переходите по ссылкам от неизвестных, не устанавливайте программы по их просьбе и не используйте чужие файлы
- Скрывайте приложения только из проверенных источников
- Обновляйте операционную систему устройства
- Используйте защищенные Wi-Fi сети