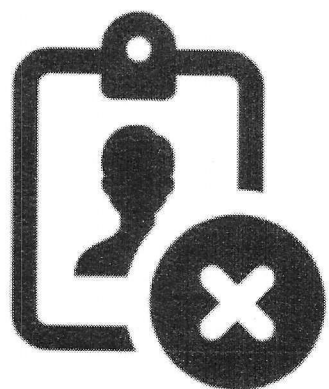


ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!



МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

- Ваша карта заблокирована
- В отношении вашей карты предпринимаются мошеннические действия
- Вашему родственнику нужна помощь или лечение
- Вам положена отсрочка по кредиту или пособию

ОН МОЖЕТ ПОПРОСИТЬ:

Данные карты:



- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

Пароль:



- от интернет-банка;
- из SMS-сообщения (для входа в интернет-банк или подтверждения операции)

Перевести деньги:



- на специальный счет или карту, где они будут в безопасности

НЕ

- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА

«ОНЛАЙН ПОКУПКИ»

Якобы продавец просит за товар предоплату либо полную оплату покупки, после чего связь с мошенником прекращается

«МЫ НАШЛИ ВАШИ ДОКУМЕНТЫ»

Якобы нашли ваши утерянные документы и просят вознаграждение за их возврат

«ПРИВЯЗКА КАРТЫ»

Просят привязать вашу банковскую карту к какому-либо номеру телефона или счёту

«ВИРУСНАЯ АТАКА»

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

«ВЫПЛАТА ПРОЦЕНТОВ»

Обещание больших процентов по вкладам под короткие сроки на различных интернет сайтах

«ПОКУПКА АВИАБИЛЕТОВ»

продажа липовых авиабилетов на мошеннических сайтах

**ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ
ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН**

ПОМНИТЕ!

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ

Помните! Ни в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счёту ни под каким предлогом!

Пользуйтесь только проверенными сайтами, на которых решили совершить какие-либо покупки!

Оплачивайте товар только после его получения!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!



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 счёта 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 присланным в SMS-сообщении с незнакомых номеров!

Никому не сообщайте ПИН-код вашей банковской карты!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!





Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ФЕДЕРАЛЬНОЕ ФИНАНСОВОЕ
СУПЕРВИЗИОННОЕ УПРАВЛЕНИЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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?

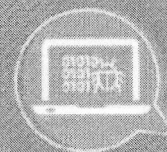
По ссылкам из интернета или электронной почты, SMS, сообщений в соцсетях или мессенджерах, рекламы, объявлений о потерях, распродажах, компенсациях от государства

! 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 проявлениях
киберугроз читайте на fincult.info



Финансовая
культура



МВД России

ОСТОРОЖНО МОШЕННИКИ

3 МИНУТЫ ОБЩЕНИЯ
КРЕДИТ НА ВСЮ ЖИЗНЬ!

НЕ СОГЛАШАЙТЕСЬ!
НИ НА ЧТО! НЕ НАЗЫВАЙТЕ ДАННЫЕ
НЕ БЕРИТЕ КРЕДИТЫ, НИКАКИХ
ДЕЙСТВИЙ НЕ ВЫПОЛНЯЙТЕ!

НЕ ВЕРЬТЕ!
ПОХОЖИМ НА БЛИЗКИХ
ГОЛОСАМ! КРИКАМ И
ПРОСЬБАМ О ПОМОЩИ

НЕ ПАНИКУЙТЕ!
ОБРАЗУ ЖЕ СБРОСЬТЕ ЗВОНКИ
И ПОЗВОНИТЕ СВОИМ БЛИЗКИМ!

НЕ ОТКРЫВАЙТЕ!
ДВЕРЬ И НЕ ВПУСКАЙТЕ В ДОМ
НЕ ПОД КАКИМ ПРЕДЛОГОМ!

ЧТО
ДЕЛАТЬ

СБРОСИТЬ
ЗВОНОК

ПОЗВОНИТЬ
БЛИЗКОМУ

ПОЗВОНИТЬ
В ПОЛИЦИЮ



РАССКАЖИ БЛИЗКОМУ



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