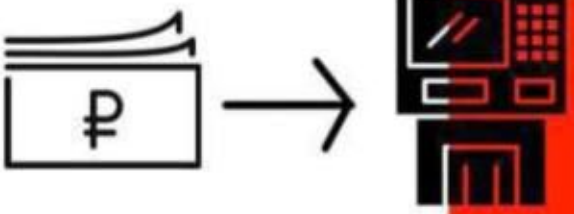
ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ЗВОНЯТ ИЗ БАНКА И СООБЩАЮТ О ПОПЫТКАХ КРАЖИ ДЕНЕГ СО СЧЕТА

ЗВОНЯЩИЙ ПРОСИТ СООБЩИТЬ ИНФОРМАЦИЮ О КАРТЕ



ИЛИ ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ СЧЕТ»

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

1. НЕ ВЫПОЛНЯЙ НИКАКИХ ТРЕБОВАНИЙ!

2. ЗАВЕРШИ ТЕЛЕФОННЫЙ РАЗГОВОР, ПОЛОЖИ ТРУБКУ!

3. ОБРАТИСЬ В БЛИЖАЙШИЙ ОФИС СВОЕГО БАНКА!

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

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА 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, 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

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!
СРАЗУ ЖЕ СБРОСЬТЕ ЗВОНОК!
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

ВИШИНГ: НОВЫЙ ВИД МОШЕННИЧЕСТВА НАБИРАЕТ ОБОРОТЫ

ЧТО ТАКОЕ ВИШИНГ?

(англ. vishing — от voice phishing)

Это вид мошенничества, когда аферисты используют телефонную связь, представляются кем-либо (например, сотрудниками банков, сотовых операторов) и выманивают у владельцев банковских карт конфиденциальную информацию.

КАК ЭТОМУ ПРОТИВОСТОЯТЬ?

Вам позвонил сотрудник банка и сказал, что мошенники пытаются похитить ваши деньги? Без паники! Просто:

КЛАДИТЕ ТРУБКУ. Это и есть МОШЕННИКИ!

Незнакомцы просят назвать код из смс-сообщений? Прочитайте внимательно СМС. В СМС написано "НИКОМУ НЕ НАЗЫВАЙТЕ КОД". Не нарушайте это правило, чтобы сохранить свои деньги.

БУДЬТЕ УМНЕЕ АФЕРИСТОВ!

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

МОШЕННИКИ

Представляются сотрудниками **СЛУЖБЫ БЕЗОПАСНОСТИ**

Присоединяйся к группе в телеграм **«МЫ ВМЕСТЕ!»:**

@rfvmeste

НЕ СООБЩАЙТЕ НИКОМУ ДАННЫЕ вашей карты

ПАРОЛЬ CVC-КОД с оборота карты и секретный код из СМС