Сотрудники Центробанка **не обзванивают** людей!

Банк России

Обещают списать долги?

Проверь, что это не мошенники!

Банк России

УМВД РОССИИ ПО АРХАНГЕЛЬСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕ

ВНИМАНИЕ!

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА

НИКОГДА

НЕ ЗВОНЯТ

ПО ПОВОДУ ПРОБЛЕМ СО СЧЕТОМ ИЛИ НЕЗАКОННОГО ОФОРМЛЕНИЯ КРЕДИТА

НЕ СОВЕРШАЙТЕ ПОД ДИКТОВКУ ОПЕРАЦИЙ, КОТОРЫХ НЕ ПОНИМАЕТЕ

НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НА ТАК НАЗЫВАЕМЫЕ «БЕЗОПАСНЫЕ» СЧЕТА - ЭТО ОБМАН!

НЕ СООБЩАЙТЕ ПОСТОРОННИМ НОМЕРА И КОДЫ БЕЗОПАСНОСТИ БАНКОВСКИХ КАРТ

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ,
НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ: 02 ИЛИ 112

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает!
Виды телефонного и интернет-мошенничества и способы защиты от них.

1. Сотрудники банков или правоохранительных органов никогда не звонят гражданам с сообщениями о проблемах с банковским счетом или попытках незаконного оформления кредита. Не предлагают перевести деньги на «безопасный» счет. Любой подобный звонок, даже если он поступает якобы с официального номера организации – дело рук мошенников!

2. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного банка, трехзначный код на обороте карты, коды из СМС. Не переходите по ссылкам в сообщениях, которые пришли от незнакомых людей по электронной почте, в соцсетях или СМС.

3. Совершая покупки в интернет-магазинах или на сайтах с бесплатными объявлениями, будьте осторожны. Отдавайте предпочтение проверенным интернет-ресурсам, использующим сервис «безопасная сделка».

4. Поступил звонок о компенсации за некачественные лекарства или медицинские приборы? Для получения денег предлагают оплатить ряд услуг? Это обман! Не переводите денежные средства незнакомым людям.

5. Звонит оператор сотовой связи и сообщает об окончании срока действия сим-карты? Это мошенник! Действие сим-карты бессрочно. Не вводите на телефоне комбинации цифр и символов под диктовку третьих лиц.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. «Родственник» по телефону сообщает, что попал в ДТП. Срочно просит крупную сумму денег. Это уловка аферистов! Прекратите разговор. Перезвоните родственнику, убедитесь, что с ним все в порядке. Не передавайте деньги посторонним людям.

8. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.

9. Нашли в сети Интернет информацию о возможности заработать на курсах акций? Будьте бдительны! Вас могут обмануть! Пользуйтесь услугами официально зарегистрированных брокерских организаций.

Если вы стали жертвой преступления, незамедлительно обратитесь в полицию по номерам телефонов: 02 (102) или 112.

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

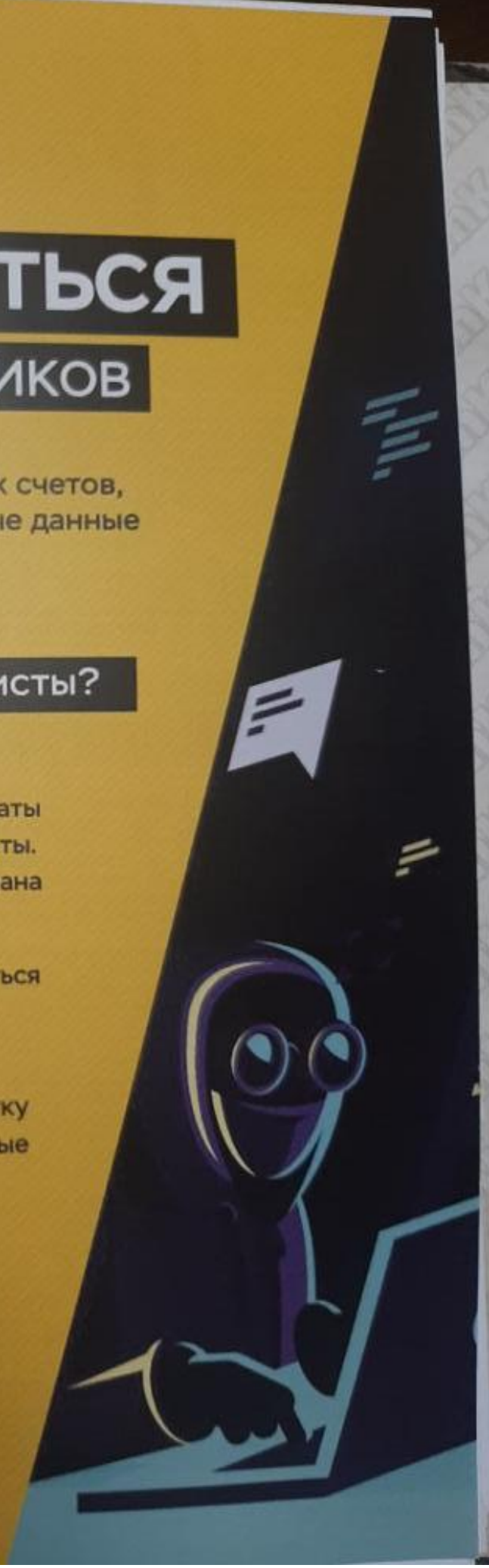
Какие схемы используют аферисты?

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



Говорят про деньги?

Клади трубку и сам перепроверяй информацию!

Банк России

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