

# ВНИМАНИЕ!

## информация о рисках мошенничества в сфере финансов и способов снижения вероятности хищения средств в результате действий злоумышленников

### 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, SMS, сообщений в соцсетях или мессенджерах, рекламе, объявлений о лотереях, распродажах, конкурсах или от родственников.

Хакеры часто выламывают чужие аккаунты, и фишинговые ссылки могут прийти даже от знакомых.



#### КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой буквинок
- В адресной строке нет https и значка закрытого замка
- Дизайн скопирован максимально точно, в тексте есть ошибки
- У сайта много страниц или даже одна – для ввода данных карты



#### КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Установите антивирус и регулярно обновляйте его.
- Сохраняйте в закладки адреса нужных сайтов.
- Не передавайте по подозрительным каналам.
- Используйте отдельную карту для покупок в интернете, кладите на нее нулевую сумму прямо перед оплатой.

### КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

#### ВИРУСЫ:

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

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов.



#### КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАИЖЕНО?

Зависит, перезагружается или опломбировано. Само замедляет работу гаджетов. Показывает всплывающие окна. Таргет объявлений.

#### ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

Позвоните в банк и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовались на устройстве. Обратиться в сервисный центр, чтобы выключить таргет. Переименовать карты, сменить логины и пароли от онлайн-банка и онлайн-установки банковских приложений.

#### КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

Использовать антивирус и регулярно его обновлять. Не скачивать не проверенные приложения, не устанавливать программы по их просьбе и не использовать чужие файлы. Своевременно проводить чистку из проверенных источников. Обновлять операционную систему устройства. Избегать общественных Wi-Fi сетей.

### ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

#### 1 ЗАБЛОКИРОВАТЬ КАРТУ



- по номеру телефона банка на банковскую карту или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

#### 2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕИСПОЛНЕНИИ С ОПЕРАЦИЕЙ



- Заявление должно быть написано
- в течение суток после сообщения в службу банка
- на месте и в отделении банка

#### 3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



«Напишите отчет, подайте заявление, вам выдадут справку, что преступника ищите!»

#### КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

##### НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и предельный код на ее обратной стороне (CVV/CVC)
- логины и коды на уведомлений
- логины и пароли от онлайн-банка

##### КОДОВОЕ СЛОВО

используйте только со стороны банка, когда сами заходите на порталы банка.

##### НЕ ПУБЛИКУЙТЕ

персональные данные и пароли доступа

##### УСТАНОВИТЕ

антивирус на все устройства



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

# 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

## Как обезопасить свои деньги в интернете?

- 1 Установите антивирус и регулярно обновляйте его
- 2 Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
- 3 Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
- 4 Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
- 5 Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на [fincult.info](http://fincult.info)



Финансовая культура

# 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](http://fincult.info)



Финансовая культура