



# 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





# НЕ ОТДАВАЙТЕ КАРТУ В ПЛОХИЕ РУКИ!



## КТО ТАКИЕ ДРОППЕРЫ

Это сообщники злоумышленников, которые выводят и обналичивают похищенные у граждан деньги.

## ЧЕМ ЗАНИМАЮТСЯ ДРОППЕРЫ

- Получают на свои карты деньги от незнакомцев и передают их другим лицам – наличными или переводом
- Предоставляют злоумышленникам банковские карты или доступ к онлайн-банку
- Принимают наличные деньги от неизвестных людей, вносят их на свои счета для последующего перевода

## ГДЕ И КАК ИЩУТ ДРОППЕРОВ

Основной канал – интернет (социальные сети, мессенджеры, электронная почта).

Злоумышленники обещают гарантированный доход без официального трудоустройства и удаленный режим работы. Опыт работы и специальные навыки их не интересуют.

Единственное требование к дропперу – наличие банковских карт.

## ЧТО ГРОЗИТ ДРОППЕРАМ

- ❗ Дропперы попадают в базу данных Банка России
- ❗ Банки ограничивают им доступ к онлайн-банку и картам
- ❗ Для многих граждан такая «работа» заканчивается уголовным наказанием



Банк России



ПРОКУРАТУРА  
СВЕРДЛОВСКОЙ  
ОБЛАСТИ

# 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

