

КАКИЕ СХЕМЫ ИСПОЛЬЗУЮТ ОНЛАЙН-МОШЕННИКИ?



Финансовая
культура

ОСТОРОЖНО: телефонные мошенники! 5 признаков обмана



Финансовая
культура

1

На вас выходят сами

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой или Центробанком.

Любой подобный звонок, СМС или письмо – повод насторожиться.

Это я, твой банк!

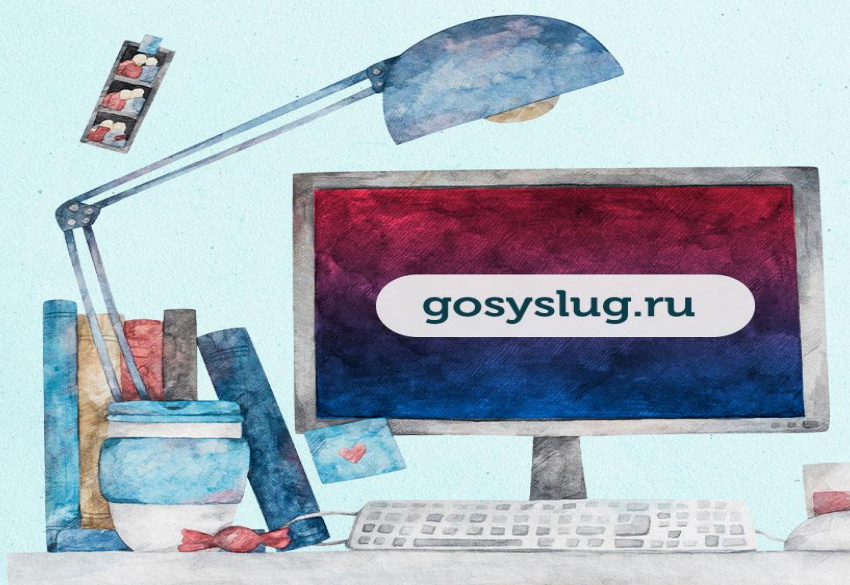


Фишинг – кража персональных данных или денег человека с помощью сайтов-подделок.

A black fishing hook is shown catching a white rectangular sign. The sign has the words 'ЛОГИН' and 'ПАРОЛЬ' written on it in large, bold, dark blue letters. The background is a light blue gradient.

**ЛОГИН
ПАРОЛЬ**

Часто мошенники делают сайты,
которые как две капли похожи
на сайты настоящих организаций.



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.



3

На вас давят

Мошенники всегда торопят, чтобы у вас не было времени все обдумать.

**Переведите
срочно!**

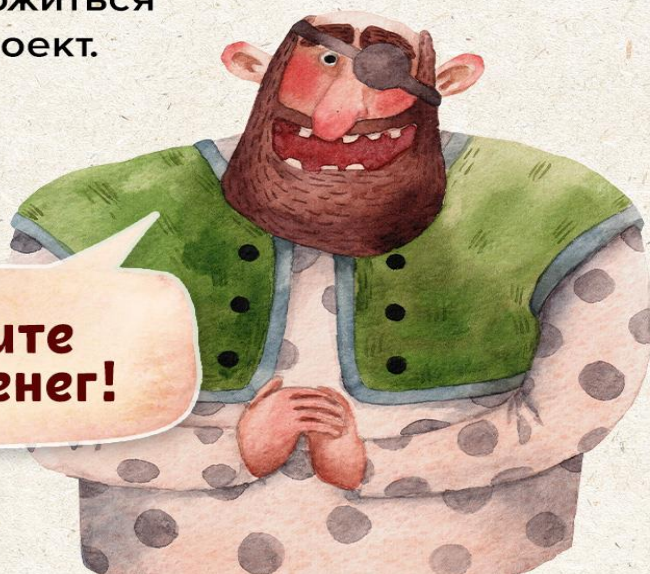


4

Говорят о деньгах

Предлагают спасти сбережения, перевести деньги на специальный счет в Центробанке, получить компенсацию или вложиться в инвестиционный проект.

Вы же не хотите остаться без денег!



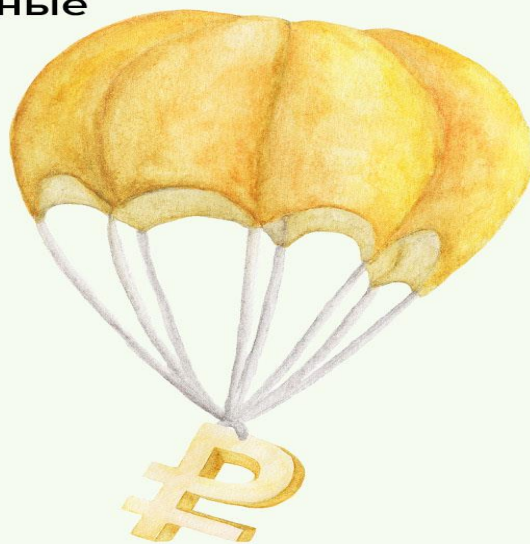
Как можно оказаться на фишинговом сайте?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях и мессенджерах, рекламы, объявлений о распродажах, лотереях или компенсациях от государства.



СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ

Например, предлагают получить государственные дотации, обещают оформить карту зарубежного банка или избавить вас от долгов.



МАСКИРУЮТСЯ

Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений.



5

Просят сообщить данные

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений.

Циферки из СМС скажете?



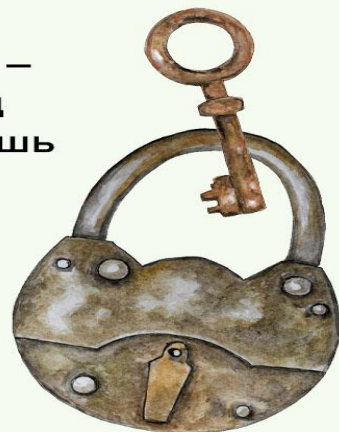
Как распознать фишинговый сайт?

1. Адрес отличается от настоящего лишь парой символов.
2. В адресной строке нет **https** и значка закрытого замка.



КАК ОБЕЗОПАСИТЬ СВОИ ДЕНЬГИ В ИНТЕРНЕТЕ?

- Установите антивирус и регулярно обновляйте его.
- Заведите отдельную карту для платежей в интернете и кладите на нее нужную сумму перед оплатой.
- Всегда проверяйте адреса сайтов – названия мошеннических страниц могут отличаться от настоящих лишь парой символов.
- Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения.



Сотрудники банков и полиции никогда не спрашивают:

- реквизиты карты
- пароли из СМС
- персональные данные

И никогда не просят переводить деньги с вашей карты!

