Слишком привлекательно,
или как распознать фишинговый сайт

Фишинговый сайт полностью или частично копирует официальный ресурс, чтобы обманом получить ваши деньги или личные данные.

еженедельно
> 100
фишинговых сайтов выявляет Сбер и инициирует блокировку

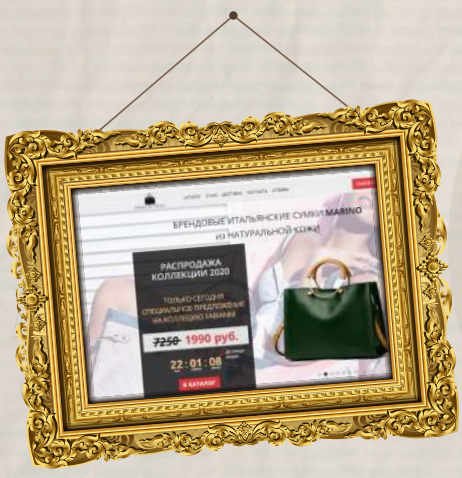
ежегодно
> 200 млн
переходов на фишинговые сайты блокирует Лаборатория Касперского

< 20%
людей читают пользовательские соглашения сайтов

> 700
фишинговых сайтов, имитирующих сайт компании криптовалютных финансовых услуг, появилось за три месяца

Мошенники умело используют психологические уловки. Самые распространенные схемы обмана на фишинговых сайтах выглядят так:

Бренд за полцены

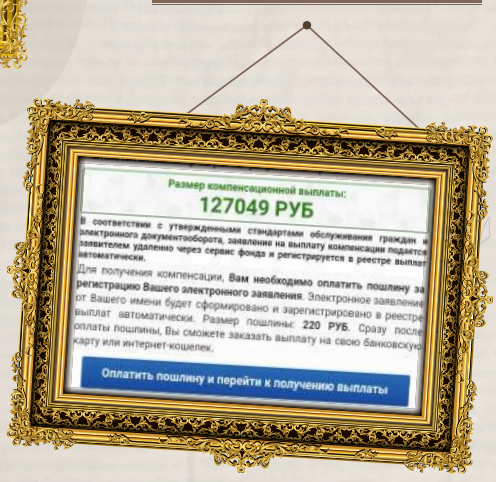


Товары известных брендов по невероятно низким ценам. Один нюанс — товар можно получить только наложенным платежом, а это значит — желанную покупку выдадут только после полной оплаты на почте. Открыв посылку, ты обнаружишь вместо редкой сумки или наушников отличный набор опилок. А деньги тебе не вернут, ведь покупку ты совершил не на почте.

О, «счастливчик»!

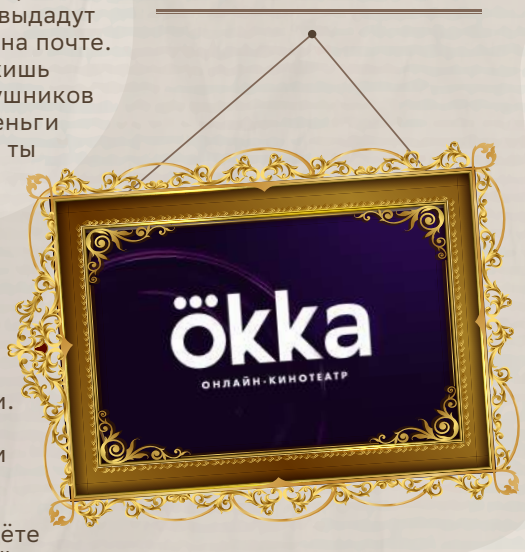
Огромный денежный приз за прохождение опроса с небольшим условием — ответить на вопросы и разослать информацию об акции в мессенджерах, а затем внести небольшую комиссию якобы для получения приза. Ты не только отдашь деньги злоумышленникам, но и поставишь под угрозу своих друзей.

Льготы и компенсации



На сайте, очень похожем на официальный, предлагается заполнить личные данные, чтобы, например, получить компенсацию за лечение, оформить пенсионные льготы или выплаты от государства. Нужно указать ФИО и, например, номер социального страхования и актуальный адрес. В итоге мошенники собирают актуальную базу данных людей с их реальными адресами и номерами соцстрахования.

Обман для киноманов



Сайты с уникальным предложением просмотра нового фильма, сериала или спортивной трансляции. Обещанная демонстрация прерывается с требованием пройти регистрацию и оплатить символическую сумму. После того как введёте на сайте данные банковской карты, с нее может списаться любая сумма, а сами данные окажутся в руках мошенников.

Где скрывается обман?

Адрес (доменное имя) сайта.

Он должен быть понятным, без дополнительных символов и странных знаков. На мошенническом сайте отсутствует безопасное соединение по https и нет иконки закрытого замка.

Как защититься?

Проверить, фишинговый сайт или нет, поможет сервис Whois (www.nic.ru/whois). Он позволяет быстро получить всю информацию о регистрации домена. Если ресурс активен менее года или зарегистрирован на физическое лицо, это повод насторожиться.

Отсутствие контактов или возможность уточнить информацию только в одностороннем порядке.

Даже если это онлайн-сервис, у него должен быть физический адрес.

Как защититься?

Обрати внимание на контакты. Оставляя свой номер для обратной связи с менеджером сайта, ты увеличиваешь шансы того,что тебе перезвонит мошенник.

Предложение, от которого сложно отказаться.

И сообщения, создающие ажиотаж и провоцирующие тебя на быстрые действия. Скорее переходи... Предложение действует до 24:00... До конца распродажи осталось 2 часа 42 минуты...

Как защититься?

И вновь золотое правило — не торопись! Постарайся трезво оценить информацию. Остаться без денег ты всегда успеешь. О реальных акциях и распродажах можно узнать на официальном сайте компании.

Оформление, дизайн сайта и грамотность изложения информации.

Некогда доводить сайт до совершенства, он же не навсегда.

Как защититься?

Следи за орфографией. Грамматические ошибки, а также небрежность в дизайне и оформлении (нестыковки в датах, названиях и изображениях) выдают фальшивый сайт.

Пользовательские соглашения, условия оплаты и доставки.

На поддельных сайтах может отсутствовать самое главное — продавец товара или услуги, за которыми ты пришёл на сайт.

Как защититься?

Внимательно изучи документы, в соответствии с которыми осуществляется деятельность компании.

Форма для ввода личных или финансовых данных.

Как защититься?

Задумайся, зачем этот сайт запрашивает номер банковской карты, паспортные данные, логины и пароли от других ресурсов? Даже для входа в личный кабинет СберБанк Онлайн не требуется такой подробной информации.

Если сайт вызывает у тебя малейшие подозрения, не пользуйся услугами этого сайта!

Подключай сервисы кибербезопасности в СберБанк Онлайн