СБЕР КИБЕР БЕЗОПАСНОСТЬ | КИБРАРИЙ

Как распознать фишинговый сайт

Злоумышленники делают фишинговый сайт похожим на официальный ресурс, чтобы обманом получить ваши деньги или личные данные

>700

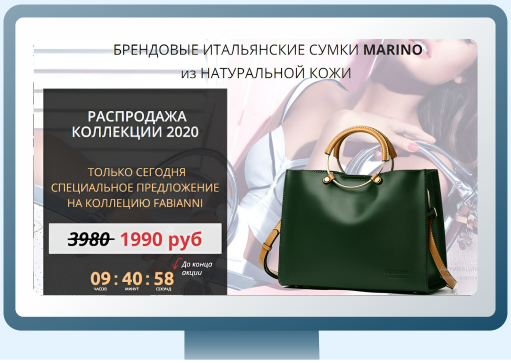
Фишинговых сайтов, имитирующих финансовых услуг, появляется каждый квартал

>100

Фишинговых сайтов ежедневно выявляет Сбер и инициирует их блокировку

<20%

Людей доходят до прочтения пользовательского соглашения сайтов

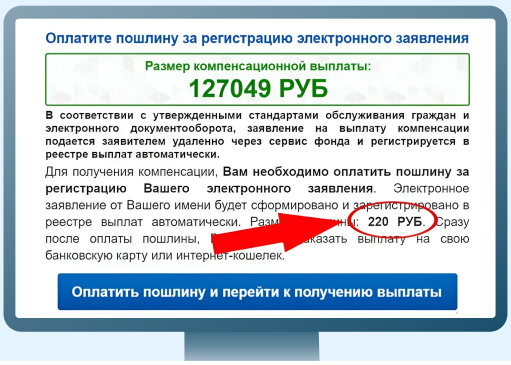


Бренд за полцены

Продажа товаров известных брендов по невероятно низким ценам. **Один нюанс:** покупку можно получить лишь наложенным платежом. То есть покупку выдадут только после полной оплаты на почте. Открыв посылку, вы обнаружите вместо редкой сумки или наушников набор опилок. А деньги почта не вернёт, ведь товар вы купили не у неё

«О, счастливчик!»

Огромный денежный приз за прохождение опроса. **Есть условие:** нужно не только ответить на вопросы, но и разослать информацию об акции в мессенджерах, а затем внести небольшую комиссию якобы для получения приза. Вы не только отдадите деньги злоумышленникам, но и подтолкнёте к этому своих друзей



Льготы и компенсации

На сайте, очень похожем на официальный, предлагается указать личные данные, чтобы получить компенсацию за лечение, оформить пенсионные льготы или выплаты от государства. Нужно будет сообщить ФИО, СНИЛС и адрес и другие личные данные. Так мошенники собирают базу данных с актуальными персональными данными

Обман для киноманов

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

Пользовательские соглашения, условия оплаты и доставки

На поддельных сайтах могут отсутствовать данные продавца товара или услуги, за которыми вы пришли на сайт.

Как защититься? Внимательно изучите документы, по которым работает компания.

Форма для ввода личных или финансовых данных

Задумайтесь, зачем этот сайт запрашивает номер банковской карты, паспортные данные, логины и пароли от других ресурсов.

Как защититься? Не вводите личные данные. Для входа в личный кабинет СберБанк Онлайн и другие сервисы не требуется такой подробной информации.

Предложение, от которого сложно отказаться

Сообщения провоцируют вас на быстрые действия: «Скорее переходи», «Предложение действует до 24:00», «До конца распродажи осталось 2 часа 42 минуты».

Как защититься? Не торопитесь — постарайтесь трезво оценить информацию.О реальных акциях и распродажах можно узнать на официальном сайте компании.

Оформление, дизайн сайта и грамотность

Некогда доводить сайт до совершенства, он же не навсегда.

Как защититься? Грамматические ошибки, небрежность в дизайне и оформлении (нестыковки в датах, названиях и изображениях) выдают фальшивый сайт.

Адрес (доменное имя) сайта

Он должен быть понятным, без дополнительных символов и странных знаков. Отсутствие безопасного соединение по https и иконки закрытого замка могут быть признаками мошеннического сайта.

Как защититься? Используйте защитное программное обеспечение с функцией предупреждения о фишинговых сайтах.

Отсутствие контактов или возможность уточнить информацию только в одностороннем порядке

Даже если это онлайн-сервис, у организации, которая его оказывает, должен быть физический адрес.

Как защититься? Обратите внимание на контакты. Оставляя свой номер для обратной связи с менеджером сайта, вы увеличиваете шансы того, что перезвонит мошенник.

Если сайт вызывает малейшие подозрения, не пользуйтесь им!

Что изучить ещё

Узнайте больше о безопасности в интернете

Больше информации — в библиотеке знаний по кибербезопасности «Кибрарий»