

Что такое фишинговые сайты

Это поддельные веб-страницы, созданные для кражи личных данных (логинов, паролей, номеров банковских карт и другой конфиденциальной информации). Такие сайты могут имитировать популярные страницы и сервисы, чтобы обмануть пользователей и заставить их ввести личные данные.

Интернет-банкинг

Социальные сети

Страницы входа в электронную почту

Онлайн-магазины

Торговые платформы

Корпоративные сайты

Личные кабинеты

Методы, которые используют мошенники на фишинговых сайтах



Поддельные формы входа.

Фишинговые сайты часто содержат формы для ввода логина и пароля, которые выглядят как настоящие, но на самом деле отправляют введенные данные мошенникам.

Имитация официального дизайна.

Сайты могут точно копировать дизайн настоящих сайтов известных брендов, финансовых организаций или сервисов.

Манипулирование URL-адресами.

Мошенники могут использовать URL, которые очень похожи на настоящие. Для этого они могут изменять всего несколько букв (*ffln.kz* вместо *ffin.kz*) или использовать другое доменное имя верхнего уровня (*например, .com* вместо *.net*).

Фальшивые предложения и акции.

Нереально выгодные предложения, высокая доходность или срочные акции, требующие немедленного ввода личных данных или платежной информации.

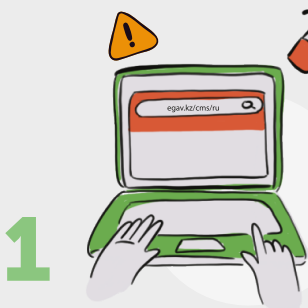
Вредоносное ПО.

Некоторые фишинговые сайты могут пытаться установить на ваше устройство вредоносное программное обеспечение под видом полезных приложений.

Скрытые перенаправления.

Посещение такого сайта может незаметно перенаправить вас на другие фишинговые или вредоносные сайты.

Как распознать фишинговые сайты



1 Проверьте URL-адрес.

Поддельные сайты часто используют адреса, похожие на настоящие, но с небольшими отличиями или опечатками.



2

Наличие HTTPS. Безопасные сайты используют HTTPS-протокол, который обеспечивает защиту передаваемых данных. Отсутствие HTTPS может быть признаком фишинга.

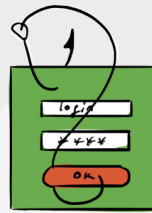
3



Дизайн и орфография.

Некачественный дизайн, грамматические и пунктуационные ошибки на сайте могут указывать на фишинг.

4



Запросы личной информации.

Будьте настороже, если сайт сразу же просит ввести конфиденциальные данные.

Как защититься

Не вводите личные данные.

Официальные сайты добросовестных компаний никогда не будут запрашивать все данные банковских карт, логины и пароли других сервисов и другие личные данные.

yes

Используйте антивирусы с функцией защиты от фишинга.

Они могут предупреждать о посещении подозрительных сайтов.

yes

Двухфакторная аутентификация. Включите ее где возможно. Так вы сможете дополнительно защитить ваши аккаунты.

yes



Всегда будьте внимательны и осторожны при вводе личных данных в интернете. Если у вас есть сомнения относительно подлинности сайта, лучше перестраховаться и не вводить данные.

Не сохраняйте пароли в браузере. Используйте надежный менеджер паролей.

yes

Регулярно обновляйте программное обеспечение. Убедитесь, что ваш браузер и операционная система обновлены до последних версий.

yes