



ПРЕЖДЕ ЧЕМ ЧТО-ЛИБО НАЖАТЬ, ДВАЖДЫ ПОДУМАЙТЕ



Вы можете потерять свои деньги, персональную информацию, а также сохранённые данные, если устройство перестанет работать. Не попадитесь на крючок!

КАК ТАКОЕ ВОЗМОЖНО?



ФИШИНГОВЫЕ АТАКИ:

Распространяются через электронную почту, текстовые сообщения, социальные медиа и выманивают персональную информацию, выдавая себя за обращения легитимных компаний, которым пользователи доверяют.



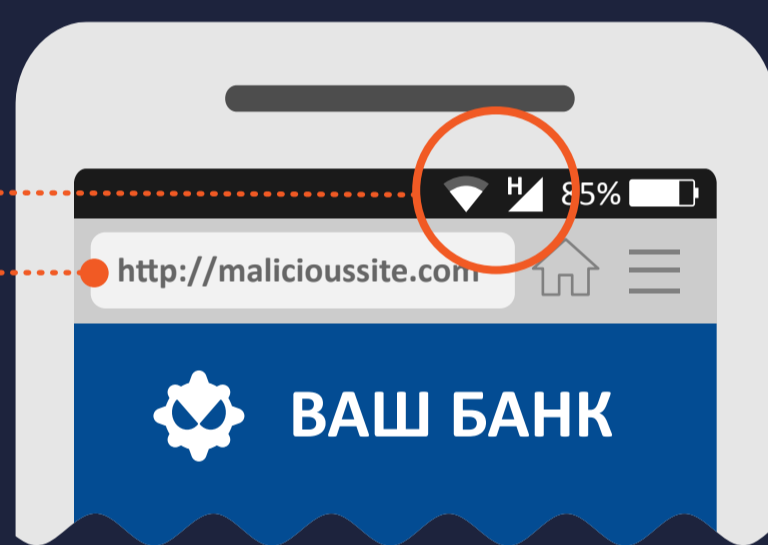
ПРОСМОТР ВЕБ-САЙТОВ: Ваше мобильное устройство может быть инфицировано просто при посещении опасного сайта.



ЗАГРУЗКА ФАЙЛОВ: Вредоносные ссылки и вложения могут содержаться непосредственно в электронном письме.

ПОЧЕМУ ЭТО СТОЛЬ ДЕЙСТВЕННО?

Мобильные устройства **ПОСТОЯННО ПОДКЛЮЧЕНЫ** к сети Интернет.



УМЕНЬШЕННЫЙ РАЗМЕР ЭКРАНА УСТРОЙСТВА — это общий ограничивающий фактор. Браузеры для мобильных устройств показывают интернет-адреса в ограниченном пространстве экрана, в связи с этим сложно проверить домен.

БЕЗОГЛЯДНАЯ ВЕРА ПОЛЬЗОВАТЕЛЕЙ в приватность мобильного устройства.

ЧТО С ЭТИМ ДЕЛАТЬ?



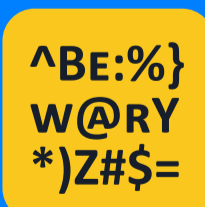
Относитесь с подозрением к SMS и звонкам от компаний, которые просят вас предоставить персональную информацию. Вы можете проверить, настоящие ли это сообщение или звонок, позвонив непосредственно по официальному номеру компании.



Никогда не нажимайте на ссылку или вложение в электронных письмах или SMS, получение которых вы не ожидали. Незамедлительно удаляйте такие сообщения.



Просматривая веб-страницы со своего мобильного устройства, убедитесь в том, что ваше соединение защищено по протоколу HTTPS. Вы всегда можете проверить так ли это, взглянув на начало интернет-адреса.



Опасайтесь, попав на сайт с плохой грамматикой, орфографическими ошибками или низкой разрешающей способностью.



Если есть возможность, установите приложение мобильной безопасности, которое будет уведомлять вас о любой подозрительной активности.