

ВИШИНГ

НЕ ОТВЕЧАЙ НА ОБМАН!

ПОМНИ:

Звонок от незнакомца — это не всегда важно.

Проверяйте информацию, прежде чем доверять или сообщать что-либо.



Вишинг — это вид телефонного мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные или деньги по телефону.

Они представляются сотрудниками банков, полиции, операторов связи и других организаций, чтобы втереться в доверие и получить доступ к вашим данным.

КАК РАСПОЗНАТЬ ВИШИНГ?

1



НЕОЖИДАННЫЙ ЗВОНОК

Вам звонят сами, хотя вы никуда не обращались. Мошенники выбирают жертв случайно.

2



ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКАМИ РАЗЛИЧНЫХ СЛУЖБ

Представляются сотрудниками банка, милиции, почты и даже поликлиники, чтобы вызвать доверие и оказать давление.

3



ПРОСЬБА СООБЩИТЬ ДАННЫЕ

Просят продиктовать пароли, коды из SMS, данные карт и паспортов или установить приложение.

4



ДАВЛЕНИЕ И СПЕШКА

Говорят, что нужно действовать срочно, иначе будут проблемы, которые повлекут за собой потерю денег.

5



ЦЕЛЬ — ВАШИ ДАННЫЕ И ДЕНЬГИ

Их цель — получить доступ к вашим личным данным и средствам, а также, возможно, похитить вашу информацию или деньги.

КАК ЗАЩИТИТЬСЯ?



ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

Перезвоните в организацию по официальному номеру, который найдете сами. Не используйте номера из SMS или сообщений.



НЕ СООБЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ

Никому и никогда не сообщайте пароли, коды из SMS и данные карт по телефону.



ПРЕРВИТЕ РАЗГОВОР

Если что-то вызывает сомнение — завершите разговор. Лучше потерять «важный звонок», чем деньги.



НЕ ПОДДАВАЙТЕСЬ НА ДАВЛЕНИЕ

Мошенники торопят вас специально, чтобы вы не успели проверить информацию и обдумать действия.



БУДЬТЕ БДИТЕЛЬНЫ

Настоящие сотрудники никогда не запрашивают конфиденциальные данные по телефону.



СТАЛИ ЖЕРТВОЙ ВИШИНГА?

Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию по телефону **102**

ФИШИНГ

НЕ КЛЮЙ НА ОБМАН!

Фишинг — это вид интернет-мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные (пароли, номера карт, логины).

Они маскируются под известные компании, банки или сервисы, чтобы заставить жертву добровольно передать ценную информацию.

ПОМНИ:

Одна ошибка — и ваш аккаунт или деньги в руках мошенников.

КАК РАСПОЗНАТЬ ФИШИНГ?

1



ПОДОЗРИТЕЛЬНЫЕ ССЫЛКИ И ОТПРАВИТЕЛИ

Проверяйте адрес отправителя и ссылки. Даже небольшая ошибка в адресе может быть ловушкой.

2



ЗАПРОС ЛИЧНЫХ ДАННЫХ

Никогда и никому не сообщайте пароли, коды из SMS и данные карты. Настоящие организации этого не требуют.

3



СРОЧНОСТЬ И ДАВЛЕНИЕ

Фразы вроде «срочно», «ваш аккаунт заблокирован» — способ заставить вас потерять бдительность.

4



ОРФОГРАФИЧЕСКИЕ И СТИЛИСТИЧЕСКИЕ ОШИБКИ

Мошенники часто делают ошибки в тексте и оформлении. Будьте внимательны!

КАК ЗАЩИТИТЬСЯ?



ПРОВЕРЯЙТЕ ИСТОЧНИКИ

Заходите на сайты только через официальные адреса и приложения.



ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ

Включите двухфакторную аутентификацию везде, где это возможно.



НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ

Не открывайте ссылки из писем и сообщений от неизвестных отправителей.



БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ

Перепроверяйте информацию и не поддавайтесь панике.



СТАЛИ ЖЕРТВОЙ ФИШИНГА?

Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию.

**ФИШИНГ
ОПАСНОСТЬ
В ИНТЕРНЕТЕ!**
ВНИМАНИЕ!
МОШЕННИКИ!