



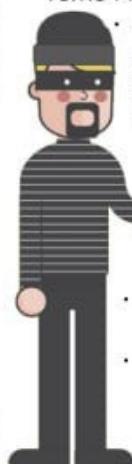
Как не стать жертвой интернет-мошенников:

- используйте для платежей отдельную карту;
- переводите на карту точную сумму денежных средств, которая необходима вам для оплаты;
- производите оплату только с защищенных антивирусами устройств;
- не используйте для расчетов устройство, к которому имеет доступ кто-то еще;
- в настройках браузеров необходимо запретить сохранение конфиденциальной информации (логины, пароли и т. д.);
- ни в коем случае не переходите по сомнительным ссылкам;
- после завершения оплаты рекомендуется выходить из браузера.

Фишинг — это когда мошенники рассылают электронные письма под видом банков, известных брендов или в социальных сетях с целью получения конфиденциальной информации.

Как не стать жертвой фишинга:

- внимательно проверяйте ссылку, на которую собираетесь кликнуть (не перепутаны ли буквы в названии сайта, нет ли неизвестных символов в наименовании сайта и т. д.);
- перед введением конфиденциальной информации (логин, пароль, данные карты), убедитесь, что соединение защищено. Если перед адресом сайта Вы увидите префикс [https](https://), это значит, что соединение защищено;
- даже если сообщение с неизвестной ссылкой пришло от лучшего друга, помните, что его тоже могли обмануть или взломать;
- если вы поняли, что вас обманывают, обязательно сообщите об этом в службу поддержки организации, работником которой представился мошенник;
- не заходите в онлайн-банки и подобные сервисы, подключившись к незащищенной точке Wi-Fi;
- вместо клика по ссылке, введите адрес сайта вручную;
- помните, что зачастую фальшивые письма и сайты, на которые ведут мошенники, во всем повторяют дизайн настоящих.



Вишиング — это когда мошенники, представляясь по телефону работниками государственных служб, банков и т. д., пытаются выманить конфиденциальную информацию у держателя платежной карты.

Как не стать жертвой вишинга:

1. Вам позвонили/прислали СМС «из банка» с неизвестного номера:

- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками государственных организаций, банков и т. д.;
- проверьте информацию, перезвонив в соответствующую организацию;
- если вы поняли, что звонил мошенник, незамедлительно обратитесь в правоохранительные органы.

2. Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- постарайтесь прервать диалог и перезвоните родным сами, узнайте всё ли хорошо.



Будьте внимательны! Не дайте себя обмануть!