Фишинг – главное оружие киберпреступников. Они выуживают не только реквизиты карты для кражи денег, но и логины и пароли от учетных записей.

Мошенники чаще всего массово рассылают электронные письма и СМС от имени банков, брендов, магазинов и даже соцсетей. В этих сообщениях содержатся специальные фишинговые ссылки, которые ведут на сайты-двойники. Преступники таким образом получают персональные данные или устанавливают на устройство жертвы вредоносные программы с целью украсть личные фото и видео.

Чтобы обезопасить себя от фишинга, не вводите свои конфиденциальные данные на незнакомых сайтах и тех, которые вызывают у вас сомнения.

Никогда не переходите по ссылкам из электронных писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать сайт.

Установите пароль на свои устройства для защиты личных данных.

Установите суточный лимит по количеству операций на своей банковской карте.

Будьте бдительны! Мошенники знают множество способов втереться к вам в доверие.