

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

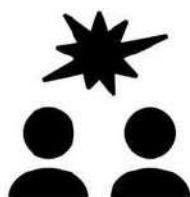


Размещать персональную и контактную информацию о себе в открытом доступе



Использовать указание геолокации на фото в постах

НЕЛЬЗЯ



Отвечать на агрессию и обидные выражения



Реагировать на письма от неизвестного отправителя



Открывать подозрительное вложение к письму



Сохрани эту информацию и поделись с другими

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:



хранить в тайне пин-код карты



прикрывать ладонью клавиатуру при вводе пин-кода



оформлять отдельную карту для онлайн-покупок



деньги зачислять только в размере предполагаемой покупки



использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций



скрыть CVV-код** на карте (трехзначный номер на обратной стороне), предварительно сохранив его



подключить услугу "SMS-оповещение"



Не рекомендуется



хранить пин-код вместе с карточкой/на карточке



сообщать CVV-код или отправлять его фото



распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"



сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure