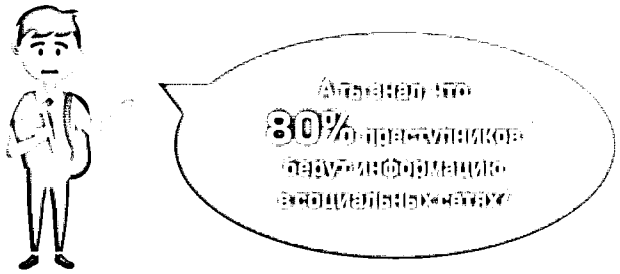
КАК НЕ СТАТЬ ИНТЕРНЕТ-ЖЕРТВОЙ?!

Общаясь в социальных сетях, будь предельно внимательным — не рассказывай подробностей своей жизни, старайся не включать в список друзей незнакомых людей. Иногда незнакомец в сети может оказаться мошенником или хакером и совершить в отношении тебя преступление — завладеть учетными данными, платежными реквизитами, персональной информацией.



ПРЕДОТВРАЩАЕМ РИСК В СОЦИАЛЬНЫХ СЕТЯХ

- регистрируйся под псевдонимом
- настрой приватность
- не делись информацией о своем местонахождении и имуществе
- не доверяй свои секреты незнакомцам из интернета

ОТКРЫТЫЕ СЕТИ. ЧУЖАЯ ТЕХНИКА

При подключении к открытой сети (метро, кафе и т.д.) ты оставляешь персональные данные, в их числе логи с паролем (если заходишь на страницу в соцсети, на электронную почту). Получив доступ к твоим персональным данным, злоумышленники могут украсть аккаунт в социальных сетях, получить доступ к электронным платежным системам или банковским картам.

ПРЕДОТВРАЩАЕМ РИСК ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТЫХ СЕТЕЙ И ЧУЖОЙ ТЕХНИКИ

- при работе с публичными устройствами используй пункт «чужой компьютер» и не сохраняй на нем свой пароль
- используй режим «приватного просмотра» в браузере
- пользуйся кнопкой «выйти» при завершении работы с ресурсами
- используй только сложные пароли и безопасные соединения

ЭЛЕКТРОННЫЕ ФИНАНСЫ

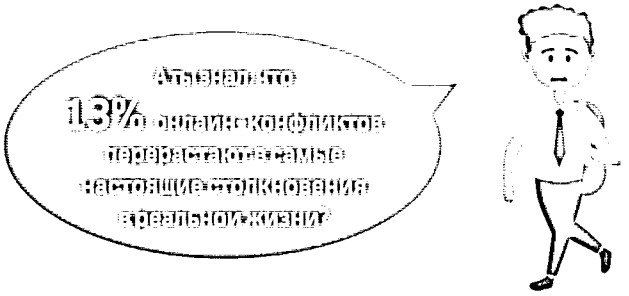
Интернет-транзакции, электронная коммерция, мобильный банкинг, кредитные карты в сети Интернет — актуальные тренды. Но будь внимательным и не пренебрегай основными правилами.

ПРЕДОТВРАЩАЕМ РИСК СТАТЬ ЖЕРТВОЙ ФИНАНСОВОГО МОШЕННИЧЕСТВА

- делай длинные и сложные пароли для платежных систем
- не переходи по ссылкам, набирай адрес сайта самостоятельно
- имя протокола должно выглядеть следующим образом: https://...
- осуществляй транзакции только на домашнем компьютере
- внимательно относись к оповещениям своего банка
- не отказывайся от SMS-оповещения! Они помогают контролировать операции
- по возможности не отключай GPS
- постарайся оборудовать телефон своими биометрическими параметрами

КИБЕРБУЛЛИНГ КАК «БОЙЦОВСКИЙ КЛУБ»

Если ты столкнулся к кибербуллингом, то обязательно сообщи об этом родителям или педагогам. Кибербуллинг может быть столь же опасным и болезненным, как и конфликт в реальной жизни.



Виды кибернападок: оскорбление, клевета, публичное разглашение личной информации, преследование, угроза физической расправы.

Помни: кибербуллинг может повлечь наступление юридической ответственности, в лучшем случае — административной.

ПРЕДОТВРАЩАЕМ РИСК СТАТЬ ЖЕРТВОЙ КИБЕРБУЛЛИНГА

- не вступай в словесные перепалки в соцсетях, форумах, даже если их участниками являются твои друзья
- чаще меняй пароли в соцсетях
- игнорируй оскорбляющие тебя сообщения и сообщи об этом взрослым
- не угрожай хулигану
- не выкладывай в сети компрометирующую тебя информацию
- добавь злоумышленника в черный список/ удали из друзей