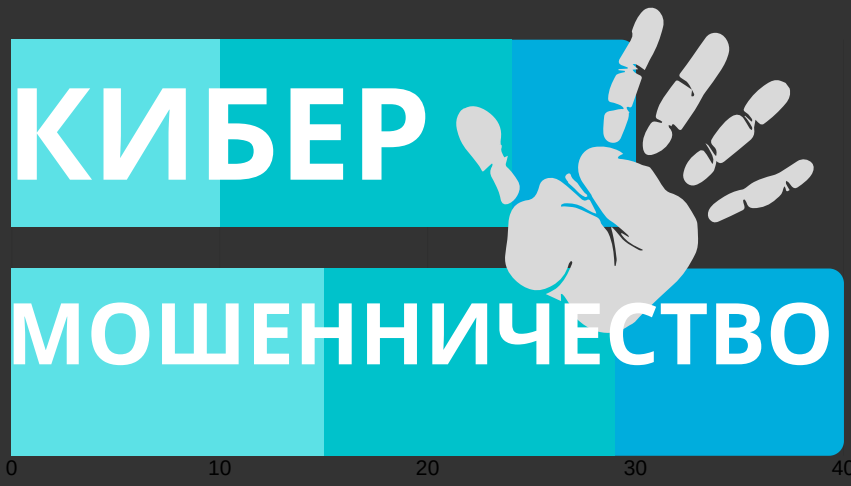
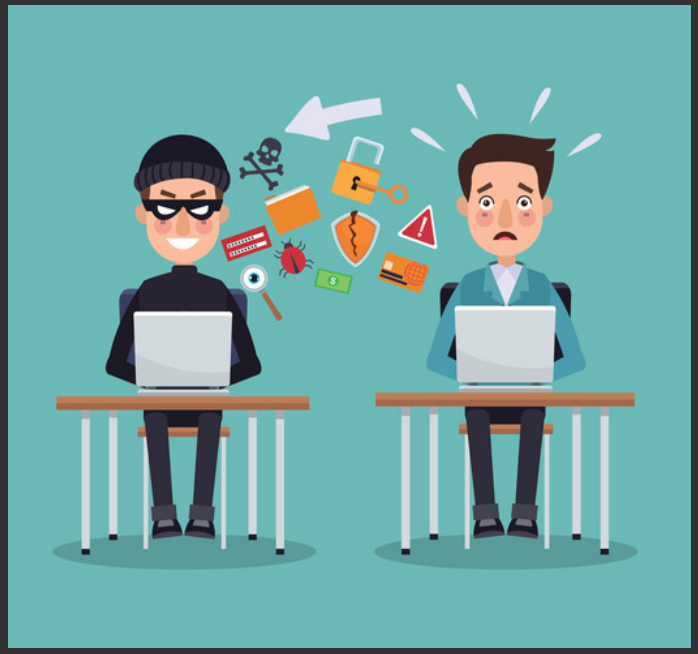
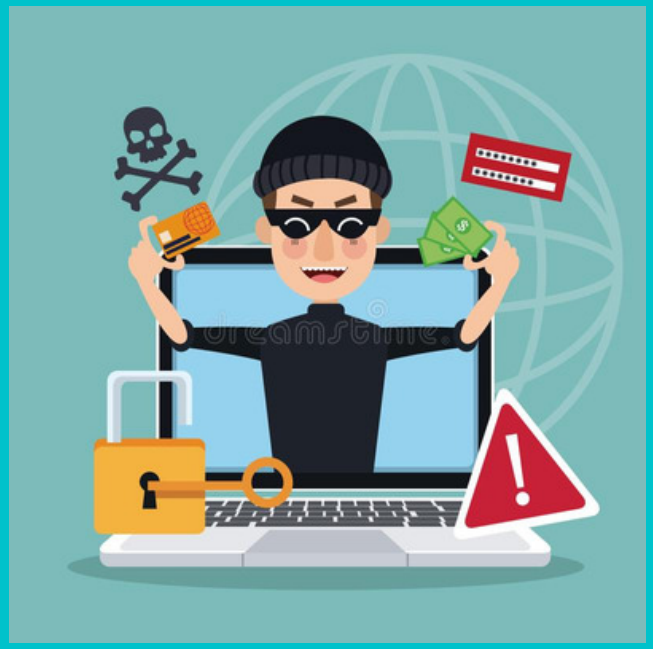
Как предотвратить кибермошенничество

- Тщательно контролируйте своё поведение в социальных сетях.
- Установите на компьютер антивирусное и антишпионское программное обеспечение.
- Для сохранности ваших учётных записей ограничьте
- Доступ к внутреннему кругу друзей
- Никогда не кликайте на сообщения, присланные на электронную почту и предлагающие обновить персональные данные
- Не используйте одинаковый пароль для разных учётных записей





Используемый источник:
https://www.colady.ru/10-metodov-moshennichestva-i-vorovstva-deneg-v-internete.html



Киберпреступность растет, этот вид деятельности стал прибыльным для жуликов и аферистов разных мастей.
Зная о рисках, вы сможете сами гораздо эффективнее, чем раньше, защищать с трудом заработанные средства от незваных гостей из сети.

ВИДЫ
КИБЕРМОШЕННИЧЕСТВА

- Фишинг - подразумевают установку вредоносного программного обеспечения на ваши устройства после того, как вы нажимаете на ссылку, полученную по электронной почте или в социальных сетях.

- Общественный интернет - Публичные сети бесплатного доступа по **Wi-Fi** опасны тем, что открывается доступ к устройству в зоне, где невозможно проконтролировать всех и каждого. Некоторые аферисты выезжают в кафе, аэропорты, считывают данные для управления мобильным банком и пользуются средствами посетителей этих точек.

- Компьютерный вирус -Вам кажется, что вы получили сигнал о вирусной атаке и надо запустить сканирование. Нажимаете на кнопку и получаете видео, имитирующее этот процесс. На самом деле, вирусное приложение в этот момент пытается заполучить ваши пароли.

СТАТЬЯ 159.6 УК РФ. МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ