



Вымогательство в сети Интернет

Будьте осторожны!



За 9 месяцев 2024 года
в полицию поступило 6,5
тысяч заявлений по
факту вымогательств в
сети Интернет.

Даже если вы кристально честный человек,
мошенники найдут, чем вас шантажировать.

А не найдут - придумают.

Чаще всего за спиной у цифровых
вымогателей нет ничего и их действия -
просто блеф.

@cyberpolice_rus



Способы вымогательства - угрозы тюрьмой за комментарии



Вымогатель следит за дискуссиями в крупных пабликах, ищет спорные комментарии и активных комментаторов, а потом пишет сообщения от лица сотрудника спецслужб. Будет предложен вариант - или деньги, или уголовное преследование.



Это не сотрудник полиции! Это мошенник! Подобные сообщения он каждый день рассылает десятками людей. Пожалуйста в поддержку соцсети на мошеннические действия и добавьте профиль вымогателя в черный список.



Способы вымогательства - выкуп за утерянную вещь



Вымогатель находит в соцсетях объявление с просьбой вернуть за вознаграждение утерянные вещи: документы, смартфоны, ключи от машины. Как вариант, злоумышленники мониторят объявления о розыске потерявшихся домашних животных.



Если вы хоть раз подавали такого рода объявления, вам наверняка писали злоумышленники с предложением сначала заплатить, а потом получить утерянное. Вознаградить за помощь - можно, но только после получения пропажи и при личной встрече.



Способы вымогательства - взломали веб-камеру



Вымогатель угрожает, что через веб-камеру заснял человека в обнаженном виде, и это видео получат все его друзья, если он не переведет деньги в течение 24 часов.



Даже если в письме нашлись ваши личные данные, это не значит, что вас взломали и записали видео с веб-камеры. Данные могли появиться у шантажиста множеством разных путей, например, из утечки. Если злоумышленник получил доступ к периферийным устройствам - лучше проверьте банковские приложения!



Способы вымогательства - штраф за просмотр запрещенного контента



Как правило, для реализации такого рода вымогательства используются баннеры на сайтах для взрослых или на сайтах с пиратским контентом. Злоумышленник копирует герб госоргана, потребует оплатить штраф.



Ни один орган государственной власти никогда не взимает штрафы подобным способом! Закройте баннер, браузер, сайт, попробуйте перезагрузить систему и ни в коем случае, не переходите по предложенным ссылкам!



Способы вымогательства - заражение вирусом шифровальщиком



Довольно распространенный способ вымогательства - заражение устройства вирусом "блокером" или "шифровальщиком". При недостаточном уровне цифровой гигиены и отсутствии антивирусных программ устройство может перестать функционировать.



От троянов-блокировщиков хорошо помогает бесплатная программа **Kaspersky WindowsUnlocker**. С шифровальщиками сначала нужно ликвидировать заразу. Следующий этап — восстановление зашифрованных файлов. Если есть резервная копия, то проще всего восстановить файлы из нее. Если резервной копии нет, можно попробовать расшифровать файлы с помощью специальных утилит — декрипторов.



Способы вымогательства - распространение интимной переписки



Вымогатель инициирует общение в сервисах знакомств, предлагает обмениваться интимными фотографиями и даже присылает их первым/ой. После получения желаемого, требует денег за удаление фото, угрожает их распространением среди ваших близких.



Такие проблемы проще предотвратить, чем решить.
Единственное, что можно сделать в такой ситуации, — это не платить и прекратить общение с вымогателем. Если заплатите, это только поможет шантажисту убедиться, что он нащупал ваше слабое место. Обязательно обратитесь в полицию!



Способы вымогательства - распространение дипфейков



Аналог предыдущего способа, вот только изображения или видео созданы с помощью нейросетей. Как вариант злоумышленник может угрожать с помощью дипфейка сделать вас соучастником преступления или подставить иным способом.



Дипфейк легко определяется в ходе криминалистических экспертиз, а ваша репутация не пострадает, потому, что от такого никто не застрахован. В случае получения сообщения предупредите близких, объясните, что на фото или видео не вы, и обратитесь в полицию.



Способы вымогательства - "слив" персональных данных



Вымогатель получает доступ к утечкам персональных данных или к устройствам жертвы, после чего обращается с угрозой выложить, например, паспорт в открытый доступ. За сохранность требует денег.



Ни в коем случае не платите! Да, скомпрометированные данные могут использованы против вас другими мошенниками, но если злоумышленник их получил - они уже есть в открытом доступе.

Напомните вымогателю об уголовной ответственности и
обращайтесь в полицию!

