Кибер-мошенники наживаются на популярности сервиса видеоконференций Zoom
https://www.vesti.ru/doc.html?id=3253527
Zoom столкнулся и с масштабной критикой — скачок популярности привлек к сервису внимание исследователей в области кибербезопасности, которые сразу обнаружили уязвимости и небрежное обращение с пользовательскими данными.

Эксперты сомневаются в безопасности Zoom
https://rg.ru/2020/04/01/eksperty-somnevaiutsia-v-bezopasnosti-zoom.html
Хотелось бы посоветовать не отказываться в текущих условиях от Zoom или любого другого подобного софта, а быть внимательнее: хакеры сейчас действительно создают поддельные домены "Zoom" и создают одноименные вредоносные исполняемые файлы.

Zoom Security Flaw нарушает безопасность пользователей
https://scienceandtech.ru/news/zoom-security-flaw-narushaet-bezopasnost-polzovatelej/
Недостаток использует уязвимость в Zoom, где веб-сервер, установленный для улучшения пользовательского интерфейса, оставляет системы открытыми для вредоносных атак.

Сервис Zoom бросил все силы на кибербезопасность. Ему нужно поддерживать 200 миллионов юзеров вместо десяти
https://medialeaks.ru/news/0204mmg-zoom-security/
Претензий у пользователей много, причём начинаются они уже на этапе установки приложения Zoom. Оно автоматически получает очень много доступа к личным данным, которые потом утекают в сеть…

«Zoom — вредоносная программа». Программисты бьют тревогу: сервис для онлайн-общения оказался не так уж прост
https://medialeaks.ru/3103lug-zoom-is-bad/
Из-за всеобщего перехода на удалёнку Zoom сейчас на пике популярности, но специалисты обнаружили, что доверять приложению не стоит.

Уязвимость софта для телеконференций Zoom позволяет любым сайтам шпионить за пользователями через веб-камеру
https://habr.com/ru/company/pt/blog/459450/
Исследователь безопасности обнаружил уязвимость в софте для проведения телеконференций Zoom. При использовании программы на компьютерах Mac, любой открытый пользователем сайт может активировать камеру на устройстве без запроса разрешения на данное действие. Сделать это можно даже в том случае, если Zoom уже был удален с компьютера.

Уязвимость в конференц-платформе Zoom поставила под угрозу более 4 млн владельцев Mac
https://www.securitylab.ru/news/499862.php
Исследователь безопасности Джонатан Лейтшу (Jonathan Leitschuh) раскрыл информацию о серьезной уязвимости в сервисе для организации видеоконференций Zoom, благодаря которой злоумышленники могут удаленно выполнить произвольный код на целевой системе.

Новая уязвимость: как Zoom крадет пароли Windows
https://www.gazeta.ru/tech/2020/04/02/13033327/zoom_windows.shtml?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews
Видеоприложение Zoom, которое стало крайне популярным из-за вынужденного карантина, постепенно превращается из необходимого инструмента в киберкошмар. Как выяснил портал Bleeping Computer, внутри сервиса обнаружена уязвимость, которая позволяет злоумышленнику похищать данные для входа в Windows, включая пользовательский пароль.

Mashable (США): забудьте про Zoom и используйте другие инструменты для видеоконференций
https://inosmi.ru/social/20200402/247181224.html
Из-за всеобщего перехода на удалёнку Zoom сейчас на пике популярности, но специалисты обнаружили, что доверять приложению не стоит. Некоторые из них даже приравнивают приложение к вирусам и предлагают альтернативу.

Хакеры пользуются возросшей популярностью Zoom, а исследователи критикуют приложение
https://xakep.ru/2020/04/01/zoom-problems/
Zoom — это рекламный бизнес в худшем его проявлении: тот, который живет за счет собранных личных данных. Еще более жутким его делает тот факт, что Zoom может собирать большое количество данных, некоторые из которых являются очень личными.

Elon Musk's SpaceX bans Zoom over privacy concerns –memo (Руководитель компании SpaceX Элон Маск запретил сотрудникам использование приложения Zoom)
https://www.reuters.com/article/us-spacex-zoom-video-commn-idUSKBN21J71H?taid=5e855eaf9a7fcd0001c4a466&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter
(Reuters) - Ракетная компания Элон Маск, SpaceX, запретила своим сотрудникам использовать приложение для видеоконференций Zoom, ссылаясь на «значительные проблемы с безопасностью и конфиденциальностью», согласно заметке Reuters через несколько дней после того, как правоохранительные органы США предупредили пользователей о безопасности популярного приложение.