СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(19.07–2.08)

2018 № 15

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(19.07–2.08)
№ 15

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

21.07.2018
Бот в Твиттере научился отслеживать лесные пожары

Компания Descartes Labs запустила бота в Твиттере, который собирает снимки с геостационарного спутника в США и отслеживает эти данные, соотнося их с хештегами к постам в социальной сети. Об этом пишут разработчики на своей странице в Medium (InternetUA).

Твиттер-бот позволяет любому человеку отслеживать распространение пожаров на территории США. Бот анализирует данные из сервиса InciWeb, собирающего информацию о стихийных бедствиях, собирает снимки со спутников из заявленных территориях из базы GOES 16. Это исследовательский спутник, который каждые пять минут присылает фотографии поверхности Земли на сервера в нескольких диапазонах, в том числе видимом и инфракрасном с разрешением до 0,5 километров на пиксель.

После этого бот создает анимацию, накладывает на карту трассы и границы, после чего публикует в твиттер с хештегами каждые шесть часов.

***

23.07.2018
Facebook строит собственный интернет-спутник «Афина»

В мае этого года сыщики из IEEE Spectrum обнаружили нечто захватывающее: по всей видимости, Facebook тайно работала над экспериментальным спутником, который мог бы транслировать интернет на Землю с использованием радиосигналов миллиметрового диапазона. На днях Facebook подтвердила Wired, что спутник «Афина» (Athena) – действительно проект Facebook, и что компания верит в технологии спутникового интернета (IGate).

«Хотя в настоящее время мы не можем рассказать ничего конкретного об этом проекте, мы полагаем, что спутниковые технологии станут важным фактором развития инфраструктуры широкополосного доступа следующего поколения и позволят обеспечить широкополосным подключением сельские регионы, где отсутствует подключение к Интернету», рассказал представитель Facebook в интервью Wired.

Wired раскопал больше информации об «Афине». Используя закон о свободе информации, ресурс получил электронные письма от FCC, в которых показали планы Facebook по запуску спутника Athena в начале 2019 года. С космической точки зрения это очень быстро.

Впрочем, одна только Athena не предоставит значительный доступ к широкополосной связи. Компании вроде OneWeb и SpaceX – которая запустила

первый интернет-спутник в феврале – надеются достичь своих целей за счет вывода тысяч небольших спутников на низкую околоземную орбиту, чтобы сформировать целые «созвездия», посылающие интернет на землю.

Весьма интересен тот факт, что Facebook предпочла спутники для вывода интернета в мир. У компании были амбициозные планы по раздаче интернета с высотных беспилотных летательных аппаратов, но проект закрыли в июне.

***

20.07.2018

В Instagram появится возможность удалять подписчиков

Как сообщает The Verge, сотрудники социальной сети Instagram тестируют новую функцию, позволяющую пользователям удалять нежелательных подписчиков (IGate).

Многие владельцы популярных аккаунтов в Instagram не понаслышке знают, что некоторое подписчики могут серьезно докучать. Другие пользователи хотели бы скрыть из чужих лент свои фото, особенно если на них неожиданно подписались все мамины подруги. Возможно, вскоре и тем, и другим станет намного проще работать с социальной сетью.

Сотрудники Instagram сообщили, что тестируют новую функцию, позволяющую удалять выбранные аккаунты из числа подписчиков, без необходимости блокировать их или закрывать собственный профиль.

Когда именно это нововведение станет доступно для всех пользователей социальной сети, пока не известно. Скорее всего, для удаления своих фото из чьей-либо ленты будет необходимо зайти в свой профиль, выбрать вкладку «Подписчики», открыть нужный аккаунт, нажать на троеточие в верхнем правом углу его страницы и активировать соответствующую команду.

С одной стороны, это довольно простой способ, с другой – производить массовые чистки таким образом будет достаточно трудоемко.

***

23.07.2018

Facebook, Google, Microsoft и Twitter объединятся для удобства пользователей

20 июля 2018 года в блоге Google была опубликована заметка, согласно которой ведущие компании объединят усилия, чтобы пользователям было проще загружать изображения с одного ресурса на другой.

Докладніше

***

24.07.2018

Пользователи WhatsApp столкнулись с новой проблемой

Судя по жалобам, которые публикуются в социальных сетях, причиной стала некорректная работа одной из функций конфиденциальности (InternetUA).

Речь идет о статусе «last seen». В настройках этой опции, которые доступны в разделе «Конфиденциальность – Последнее посещение», можно выбрать, кто именно будет видеть, когда пользователь был онлайн. Это могут быть все, только люди из контактов или никто.

По словам пользователей, даже при установке опции «Никто» люди из списка контактов все равно могли видеть информацию о времени их последнего появления онлайн. Ошибка проявлялась в веб-версии WhatsApp, а также в приложении для Android.

***

24.07.2018

Девять скрытых функций Instagram, о которых вы могли не знать

Даже если вы установили Instagram на свой телефон, вы, вероятно, не знаете все, на что он способен. В данной статье рассказано о десяти скрытых функциях приложения, которые вы можете использовать как на Android, так и на iOS.

Докладніше

***

25.07.2018

YouTube готовит новую функцию для влогеров

Новая функция будет полезна в первую очередь блогерам. Как сообщают источники, функция «Исследование» появится в ближайшее время (IT новости).

Новый аналитический инструмент позволить оптимизировать многие процессы. В настоящее время на YouTube предпочтения измеряются только лайками и просмотрами. Функция займется анализом истории просмотров пользователей. На основании данных, сделанных после выборки, пользователям будут предлагать новые видеозаписи для просмотра.

Оценить пользу новой функции смогут, как влогеры, так и обычные пользователи.

***

30.07.2018

Веб-версия YouTube начала адаптироваться под вертикальные видео

Самый популярный в мире видеохостинг окончательно смирился с популярностью вертикальных видео. Ещё раньше YouTube добавил их поддержку в мобильные приложения, а теперь она появилась и веб-версии

сервиса вместе с новым плеером, который в целом лучше подстраивается под разные соотношения сторон. Теперь если запустить на сайте YouTube вертикальное видео, то оно автоматически подстроится под размеры плеера и будет показываться без чёрных полос по бокам (IGate).

При этом новый плеер также лучше работает с видео, у которых соотношение сторон 16:9, используя свободное пространство, чтобы увеличить картинку.

Возможно, теперь вертикальные видео, получившие огромную популярность благодаря таким сервисам, как Instagram и Snapchat, будут меньше раздражать зрителей с YouTube.

***

31.07.2018

WhatsApp запустил групповые видеозвонки для всех пользователей

WhatsApp обновил свой сервис обмена сообщениями. В мессенджере появилась поддержка групповых видеозвонков, позволяющая общаться с тремя другими людьми одновременно в приложениях для iOS и Android (IGate).

Чтобы использовать новую функцию, вам для начала нужно начать обычный голосовой или видеозвонок с одним контактом, а затем нажать кнопку «добавить участника» в верхнем правом углу экрана.

WhatsApp заявляет, что видеовызовы шифруются по принципу end-to-end – также, как и обычные текстовые сообщения.

***

1.08.2018

Как включить ночной режим в YouTube на Android

Приложение YouTube для Android получило поддержку тёмной темы оформления – так называемый ночной режим. Он активируется в настройках приложения (InternetUA).

Ранее ночной режим появился в веб-версии YouTube, а также у приложения на iOS. После его активации фон, который прежде был белым, становится тёмно-серым. Некоторые элементы также меняют окрас и меньше раздражают зрение, особенно в тёмное время.

Оформление каналов при переключении на тёмную тему не меняется: фоновые обложки остаются такими же яркими, как были, они не затеняются, и цвета на них не инвертируются. Некоторые каналы уже оптимизировали своё оформление таким образом, чтобы одинаково хорошо выглядеть с обычной и тёмной темой.

***

2.08.2018

Facebook готовит «шоу талантов»

Пользователь Джейн Манчун Вонг обнаружила новую функцию Talent Show («Шоу талантов») в коде приложения Facebook. Она позволит юзерам исполнять популярные песни на камеру, а сами ролики после записи смогут получить оценки от аудитории (InternetUA).

Вонг нашла упоминания таких элементов, как «прослушивание» и «сцена», а также интерфейс, позволяющий выбирать трек из списка известных музыкальных композиций. Нажав на нужную, пользователь может начать запись выступления. Девушка отметила, что Talent Show больше похоже на сочетание соцсети Musical.ly и серии «Пятнадцать миллионов заслуг» из сериала «Чёрное зеркало».

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

26.07.2018

МІП: Через Facebook діти можуть звернутися на «гарячу» лінію за допомогою

26 липня 2018 року в ІА «Укрінформ» відбувся круглий стіл «Безпека дитини в Інтернеті», організований Міністерством інформаційної політики України спільно з ГО «Ла Страда Україна». Учасники дискусії обговорили, які сучасні загрози чекають на дітей в Інтернеті, як убезпечити від них юних користувачів і куди можна звернутися за допомогою в мережі.

Докладніше

***

31.07.2018

У соцмережі почали збирати підписи за відставку Аласанії з посади директора Національної телекомпанії

У соцмережі Facebook розпочався збір підписів під зверненням до Наглядової ради ПАТ «Національна суспільна телерадіокомпанія України» із вимогою звільнити Зураба Аласанію з посади генерального директора (Главком). Відповідний допис – звернення від представників громадськості – розмістив у себе на сторінці український історик Олександр Палій.

Причиною вимоги відставки Аласанії стало ігнорування телеканалом «UA:Суспільне» трансляції хресного ходу за помісну церкву. «Звертаємо Вашу увагу на те, що у ході Московського патріархату, що відбулася напередодні, брали участь лідери політичних сил та народні депутати. І це не завадило ПАТ «НСТУ» висвітлювати ці заходи в значно більшому обсязі, ніж численнішу

ходу за створення Помісної православної церкви», – наголосив Палій. Як повідомлялось, сам Аласанія пояснив відсутність трансляції хресного ходу так: Україна є світською державою і церква відділена від неї і всі релігійні організації є автономними, а більшість жителів України не є вірянами чи прихожанами тієї чи іншої церкви взагалі.

***

23.07.2018

Достаточно знать госномер: в Украине запустили уникальный мессенджер для водителей

В Украине запустили приложение, которое позволит написать автовладельцу сообщение, имея в распоряжении только его номер регистрации автомобиля (InternetUA).

Молодой украинский стартап Autogram поможет с легкостью написать любому владельцу автомобиля, и он получит это сообщение, если зарегистрирован в системе. Для регистрации в уникальном мессенджере нужен номер телефона и госномер автомобиля.

Номер телефона используется только для регистрации и экстренного сообщения, другие пользователи не видят номера телефонов пользователей. Таковы правила приложения.

Все данные и переписка хранятся в зашифрованом виде на серверах предоставленных компанией Google. Анонимность – задача номер один в данном приложении.

На случай угроз и оскорблений от буйных водителей в приложении реализован черный список.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

22.07.2018

Facebook прекратил сотрудничество с фирмой, которая могла передавать данные властям

Facebook приостановила сотрудничество с американской фирмой, которая имела контракты с правительством США и другими странами, и изучает случаи возможного нарушения ею правил соцсети, касающихся передачи данных пользователей третьей стороне.

Докладніше

***

23.07.2018

Facebook разрешил рекламу Coinbase

Крупнейшая в мире социальная сеть Facebook добавила американскую компанию Coinbase в список одобренных рекламодателей (InternetUA).

Еще в конце прошлого месяца в Facebook заявили, что для получения разрешения на публикацию рекламы продуктов и услуг в сфере криптовалют рекламодатели должны предоставить данные о лицензиях, листинге на фондовых биржах и любую важную публичную информацию о своем бизнесе. Тем самым полный запрет был существенно ослаблен.

***

26.07.2018

Илья Кабачинский

Капитализация Facebook обвалилась на $150 млрд после публикации квартального отчета. Столько стоит весь Netflix

Компания Facebook Марка Цукерберга 26 июля представила финансовый отчет за квартал. Он оказался не так хорош, как того ожидали аналитики. На фоне постоянных скандалов вокруг соцсети, стоимость акций компании и капитализация Facebook драматически обвалились всего за несколько часов (AIN.UA).

Как сообщает TechCrunch, в последнем квартале пользовательская база выросла всего на 1,54 %, тогда как кварталом ранее этот показатель составлял 3,14 %. Число активных пользователей также выросло минимально. Общее число пользователей, как пишет Quartz, достигло 2,23 млрд, хотя аналитики ждали цифру в 2,25 млрд. Не удалось компании показать и финансовые результаты на уровне ожиданий аналитиков: $13,2 млрд вместо $13,3 млрд. В целом Facebook впервые за много лет не смогла оправдать прогнозы аналитиков.

Несмотря на заявления Марка Цукерберга, что деятельность Facebook не ограничивается одним кварталом, а хотя бы одним из продуктов компании пользуется уже 2,5 млрд человек, акции и общая капитализация Facebook рухнули. Всего за пару часов стоимость акций упала с $217 до $166 за единицу, а общая капитализация компании упала на $150 млрд. Для сравнения – столько же стоит весь Netflix.

Как отмечают журналисты The Washington Post, падение могло быть спровоцировано также скандалами вокруг социальной сети Facebook, а также новыми правилами GDPR в Европе, что потребует от Facebook дополнительных средств для ведения бизнеса в этом регионе.

***

28.07.2018

Борьба с нарушителями привела к падению аудитории Twitter

Twitter опубликовал отчёт по итогам второго квартала, завершившегося 30 июня 2018 года. Выручка выросла на 24 % год к году и составила $711 млн. 84,5 % ($601 млн) выручки пришлось на рекламу.

Докладніше

***

31.07.2018

Facebook откроет штаб-квартиру в Лондоне

Ведущие технологические компании расширяют присутствие в Лондоне, рассматривая город в качестве лучшего места для своей работы. Об этом сообщила в понедельник газета The Times (InternetUA).

Компания Facebook объявила о строительстве новой штаб-квартиры в районе Кингз-кросс площадью более 55,7 тыс. кв. м, отмечает издание. По словам главы отделения компании в Северной Европе Стива Хэтча, она «инвестирует в мегаполисе на долгосрочную перспективу». Великобритания – «одно из лучших мест в мире для технологичных компаний», считает он.

По данным агентства недвижимости Savills, начиная с третьего квартала 2016 года технологические компании заняли в общей сложности почти 288 тыс. кв. метров площади, или 12,8 % от всей имеющейся. «Многие крупные международные фирмы не считают, что Brexit существенно отразится на проведении бизнес-операций», – отмечает глава агентства Пол Беннет. Американские компании продолжают отдавать предпочтение Соединенному Королевству из-за общего языка, доступности венчурного капитала, меньшего, чем, например, во Франции регулирования рынка труда, а также благоприятного для стартапов налогообложения, добавляет издание.

***

2.08.2018

Бизнесу придется платить за размещение постов в популярном мессенджере

Мессенджер WhatsApp ввел функцию отправки платных сообщений для компаний, чтобы «в чатах не было беспорядка» (Payspace Magazine).

Услуги отправки некоторых сообщений будут платными для компаний, таким образом, компании будут избирательны в том, какие сообщения отправлять, а в ваших чатах не будет беспорядка

Как пояснили разработчики, после запуска приложения WhatsApp Business пользователи сообщали, что стало намного проще и удобнее написать компании в чате, чем совершить звонок или отправить электронное письмо. Таким образом, WhatsApp предоставил еще больше возможностей для компаний.

Теперь клиенты могут связаться с компаниями несколькими способами: запросить необходимую информацию, оставив свой номер телефона на их

сайте; начать чат через значок прямой связи на сайте компании; обратиться в службу поддержки.

Со временем мессенджер будет увеличивать количество компаний, представленных в WhatsApp.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

29.07.2018

Месяц без соцсетей: пользователей призывают вернуть контроль над своей жизнью

Сторонников соцсетей призывают «вернуть контроль над своей жизнью» и на целый месяц перестать «зависать» в соцсетях (InternetUA).

«Королевский союз общественного здравоохранения (RSPH) инициировала “Сентябрь без соцсетей” для пользователей Facebook, Instagram, Twitter и Snapchat», – отмечается в сообщении.

Британские специалисты убеждены, что отказ от соцсетей может положительно повлиять на сон, отношения и общее состояние здоровья, в частности на психику.

Кампания призывает тех, кто не может оторваться от мобильных телефонов, на некоторое время отказаться от них или, по крайней мере, меньше сидеть в соцсетях.

Исследование, проведенное RSPH, показало, что половина пользователей в возрасте 18-34 года считают, что полный отказ на месяц хорошо повлияет на их сон и отношения в реальном мире. Почти половина опрошенных (47 %) считает, что это окажет положительное влияние на их психическое здоровье.

Организация дает советы, как уменьшить вредную привычку. Среди них: делать перерыв от соцсетей во время каких-либо мероприятий или встреч, не пользоваться соцсетями после 18:00, не проверять собственные аккаунты в соцсетях во время учебы или работы, избегать соцсетей в спальне.

***

29.07.2018

У кіберполіції назвали найнебезпечнішу соцмережу для дітей в Україні

Російська соціальна мережа «ВКонтакте» становить найбільшу загрозу для українських дітей, заявив начальник відділу протидії злочинам у сфері обігу протиправного контенту і телекомунікацій кіберполіції Заур Урусов, пише «Детектор медіа» (InternetUA).

Хоч більшість провайдерів, які працюють на території України, вже заборонили доступ до «ВКонтакте», соцмережа залишається популярною серед підлітків.

У кіберполіції кажуть, що ця заборона ускладнила роботу їхнім слідчим, адже тепер користувачі заходять туди через VPN і злочинців значно важче вираховувати.

Тому слідкувати за своїми дітьми просять батьків. Зробити це можна за допомогою спеціальних програм батьківського контролю, підказують у кіберполіції.

Серед загроз, з якими дитина може зіткнутися в мережі, – кібербулінг (цькування онлайн), секстинг (обмін повідомленнями сексуального характеру), доведення до самогубств у «групах смерті» на кшталт «Синього кита», грумінг (входження в довіру з метою подальшого статевого акту, шантажу чи сексуальної експлуатації) або ж звичайне шахрайство.

***

2.08.2018

«Экранное время» поможет побороть зависимость от Facebook

Facebook добавила в свое приложение функцию «Экранное время», которую ранее представила Apple. Она позволяет просматривать свою активность в социальной сети – сообщает Cult of Mac (Украинский телекоммуникационный портал).

Таким образом компания хочет уменьшить количество зависимых от интернета людей. Предполагается, что статистика ужаснет пользователей и побудит их использовать Facebook реже: «Мы разработали эти инструменты на основе сотрудничества и вдохновения со стороны ведущих экспертов и организаций в области психического здоровья, ученых, наших обширных исследований и отзывов нашего сообщества», – говорится в пресс-релизе компании.

В ближайшее время доступ к функции получат все пользователи Facebook и Instagram. Она находится в настройках, в разделах «Ваше время в Facebook» в первом случае и «Ваша активность» во втором. Помимо возможности просматривать количество потраченного на соцсеть времени, можно установить оповещение, напоминающее о необходимости закрыть приложение при чрезмерном использовании Facebook. Вероятно, с помощью этой функции руководство Facebook пытается восстановить репутацию компании.

20.07.2018
Ирина Фоменко
Facebook обещает начать борьбу с насилием

Facebook начнет удалять ложные и подстрекательские публикации, которые могут спровоцировать насилие, поскольку компания столкнулась с критикой за реакцию на межконфессиональные конфликты в таких странах, как Мьянма и Шри-Ланка. Об этом сообщает The Washington Post (InternetUA).

Согласно информации Facebook, новые меры коснутся письменных публикаций и фейковых изображений. Группы гражданского общества и агентства по угрозе безопасности входят в число партнеров, которые, по словам представителей компании, помогут платформе отмечать подстрекательские посты и анализировать их потенциальное воздействие. Партнеры Facebook должны проверять, является ли информация ложной или подстрекательской. Как только угроза будет подтверждена, Facebook удалит контент и похожие публикации.

Как заявил Марк Цукерберг, Facebook видит разницу между информацией ложной и такой, что может привести к физическому вреду. В то время как Facebook не планирует запрещать Infowars, издание, известное распространением теорий заговора, социальная сеть будет удалять публикации, подстрекающие к насилию. В качестве примера Цукерберг привел жителей Мьянмы и Шри-Ланки, где социальные СМИ, возможно, способствовали смертельному сектантскому конфликту.

«Сокращать распространение дезинформации – это правильный баланс между свободой слова и безопасным сообществом», – говорится в заявлении Facebook. В компании добавили, что изменение политики позволит Facebook удалять публикации, способствующие нанесению физического вреда.

***

23.07.2018
Фальшивое сообщение в WhatsApp вновь заставило толпу линчевать невинную женщину

Еще одна женщина из Индии стала жертвой толпы, которая получила фейковое сообщение о похищении детей. Ее труп обнаружили недалеко от леса в штате Мадхья-Прадеш, сообщает South China Morning Post (InternetUA).

Полицейские сообщили, что произвели арест девяти подозреваемых в избиении потенциальной похитительницы. Обвиняемые рассказали стражам порядка, что они увидели подозрительно передвигающуюся женщину 21 июля. В тот же момент все они получили сообщение в WhatsApp о бандах преступников, орудующих в том же районе, и накинулись на прохожую.

«Мы пытаемся идентифицировать жертву и распространяем ее фотографии во все полицейские участки», – заявил начальник местного отдела полиции Рияз Икбал (Riyaz Iqbal).

В Индии WhatsApp используют более 200 миллионов человек. За последние два месяца местные жители растерзали более 20 невинных жертв из-за распространения фейковых сообщений. Индийское правительство обратилось к разработчикам с требованием исправить ситуацию и пресечь распространение фальшивых посланий.

В результате представители сервиса подключили новую функцию, которая должна автоматически предупреждать пользователей, если сообщение было скопировано или переслано. Однако даже после обновления приложения убийства не прекратились.

***

1.08.2018

«Об этом не написало ни одно СМИ». Пользователи Facebook троллят людей, которые бездумно репостят картинки

Пользователи Facebook публикуют в соцсетях фейковые картинки с призывом поддержать репостом, чтобы потролить людей, которые не проверяют правдивость информации. Их репостят десятки тысяч раз (InternetUA).

22 июля пользователь Facebook Дмитрий Коваленко опубликовал фотографию украинского боксера Александра Усика с призывом поддержать его, поскольку «СМИ молчат». Его сообщение репостнули 59 тысяч раз.

Сообщество Киев Public продолжило флешмоб и опубликовало фейковую историю про вымышленного доктора и прикрепило к ней картинку с известным мемом Гарольдом, который скрывает боль – 3 тысячи репостов.

Для того, чтобы собрать десятки тысяч репостов не обязательно кого-то поддерживать, можно просто нарисовать радугу и придумать подпись – 48 тысяч репостов.

***

1.08.2018

В Facebook сообщили об удалении десятков подозрительных страниц перед выборами в США

Руководство социальной сети Facebook уведомило американские власти, что выявило и удалило десятки аккаунтов, которые отличались «скоординированным недостоверным поведением». Об этом говорится в сообщении компании (InternetUA).

Отмечается, что из социальных сетей Facebook и Instagram удалены 32 страницы и аккаунта. По словам руководства соцсети, данные страницы

обманывали пользователей, а ведущие их лица скрывали свои личные данные и цели действий.

В соцсети подчеркнули, что обнаруженные страницы и аккаунты были связаны с протестами, которые запланированы в Вашингтоне на следующей неделе. В данный момент в Facebook не смогли установить, кто стоит за этими аккаунтами.

В ноябре нынешнего года в США пройдут выборы в палату представителей в конгрессе.

***

30.07.2018

У парламенті Британії кажуть, що фейкові новини витісняють справжні

В Інтернеті масово поширюється дезінформація, а «fakenews» починають витісняти справжні новини. Про це заявив голова комітету Палати громад британського парламенту Даміан Коллінз, пише ВВС Україна (Рубрика).

За його словами, люди нині вже ледве відрізняють фейкові новини від реальних. У доповіді комітету йдеться, що ця проблема є серйозною загрозою демократії. У ньому також міститься заклик жорсткіше регулювати соціальні мережі. Члени комітету розглянули дані щодо різних країнах світу, в яких були спроби вплинути на вибори через соцмережі.

Парламентарям надали інформацію про дії російських спецслужб щодо маніпуляції виборцями через рекламу в Facebook.

«Якщо ці інструменти втручання настільки сильні, що можуть проникати в свідомість мільйонів людей у всьому світі шляхом натискання кнопки, якщо ними можна користуватися для поширення дезінформації без розкриття її джерела, то ми маємо справу з серйозною загрозою нашій демократії», – заявив Даміан Коллінз.

Особливу увагу комітет звернув на роль британського підприємця Аррона Бенкса, який зробив найбільше у британській історії пожертвування до фонду прихильників Brexit в розмірі 8,4 млн фунтів.

У доповіді комітету наголошується, що залишається незрозумілим, звідки у Бенкса з’явилися такі гроші, а також те, що він не зумів довести зв’язок цих грошей з його активами в Британії.

«Аррон Бенкс, мабуть, прагне приховати масштаб своїх зв’язків з Росією, які включали обговорення потенційних угод у сфері видобутку золота й алмазів», – наголошується в доповіді комітету.

Спецслужби і технології «соціального контролю»

20.07.2018

Facebook отказался удалять сообщения с отрицанием Холокоста

Facebook не будет удалять сообщения пользователей с отрицанием Холокоста. Об этом основатель соцсети Марк Цукерберг рассказал изданию Recode (InternetUA).

«Я еврей, а есть группа людей, которые отрицают, что Холокост был. Меня это глубоко оскорбляет, но не считаю, что наша платформа должна убирать подобные сообщения. Я думаю, что есть вещи, о которых некоторые люди неверно осведомлены, но не думаю, что они ошибаются намеренно», – сказал он.

«Сложно подвергнуть сомнению чье-то намерение и понять его. Я не думаю, что в Facebook должны быть люди, которые решают, что является правдой, а что нет. У вас может быть страница в соцсети, и, если вы не хотите причинить урон кому-либо и не нападаете на кого-либо, тогда вы можете разместить этот контент, даже если люди могут с ним не согласиться или же найдут его оскорбительным», – пояснил Цукерберг.

В 2017 году суд австрийского города Фельдкирх приговорил мужчину, отрицавшего холокост, к 12 месяцам тюрьмы условно. На своей странице в Facebook осужденный написал, что массовые убийства евреев в газовых камерах, проходившие по приказу Гитлера во время Холокоста, – история, выдуманная самими евреями. «Таким образом подсудимый нарушил антинацистские законы Австрии», – говорится в постановлении суда.

***

23.07.2018

США создали группу для «устранения российских угроз в киберпространстве»

Глава киберкомандования США генерал Пол Накасоне заявил, что в ведомстве была создана специальная рабочая группа по противодействию России в киберпространстве (InternetUA).

Об этом генерал заявил на форуме по безопасности, который прошел в Аспене, штат Колорадо. Он отметил, что Россия обладает большими возможностями в киберпространстве, которым США «необходимо противостоять».

«Я создал российскую группу, небольшую. Это укладывается в то, что разведывательное сообщество (США) делает с 2016–2017 годов», – сказал Накасоне.

***

23.07.2018

Кремль поручил разобраться с недовольными жителями в соцсетях

Кремль инициировал запуск новой системы мониторинга «Инцидент менеджмент», которая позволит отслеживать информационные поводы в

социальных сетях и реакцию на действия властей. Об этом сообщает РБК со ссылкой на источники в Кремле и региональных правительствах (InternetUA).

По их словам, систему разрабатывало ООО «Медиалогия». В компании подтвердили информацию о разработке и поставке ее в ряд российских регионов.

Отмечается, что «Инцидент» мониторит по ключевым словам пять социальных сетей: «ВКонтакте», Facebook, Instagram, Twitter и «Одноклассники». Результаты мониторинга попадают к администратору, который решает, на какие сообщения нужно ответить. Запросы сортируются в зависимости от масштаба проблемы, посты одной темы объединяются в один кейс. По словам регионального чиновника, местные власти должны реагировать на запрос в течение суток с момента его регистрации.

Собеседник издания близкий к Кремлю рассказал, что необходимость уделять больше внимания негативным комментариям в соцсетях возникла после трагедии и кемеровском торговом центре «Зимняя вишня» и ситуации вокруг мусорного полигона в Волокамске. По словам источника, власти регионов продемонстрировали неспособность адекватно реагировать на недовольство в интернете. Сейчас система тестируется в десяти регионах.

***

23.07.2018

Чоловіку за проросійські пости в соцмережі дали 6 років тюрми

Мешканця Луцька за антиконституційні публікації в соціальній мережі «ВКонтакте» засудили до 6 років позбавлення волі (InternetUA).

Про це повідомили у Луцькому міськрайонному суді.

Суддя Василь Ковальчук проголосив вирок у кримінальному провадженні та засудив до шести років позбавлення волі лучанина, який впродовж 2014 року розміщував антиконституційні публікації у соціальній мережі «ВКонтакте», які містили «проросійські» напрями.

У своїх постах чоловік публічно закликав до зміни меж території та державного кордону України, повалення конституційного ладу, захоплення державної влади насильницьким шляхом та розв’язування воєнного конфлікту.

***

24.07.2018

Facebook и Instagram станут активнее блокировать аккаунты малолетних пользователей

Детям в возрасте до 13 лет станет ещё сложнее пользоваться Facebook и Instagram. Им и раньше было запрещено пользоваться двумя этими социальными сетями, но компания проверяла аккаунты только тогда, когда кто-то оставлял жалобу. Теперь модераторы будут блокировать учётные записи детей при каждом удобном случае (InternetUA).

Если пользователя заблокируют, но на самом деле окажется, что ему больше 13 лет, то ему придётся предоставить Facebook снимок документа, подтверждающего его возраст. Представитель социальной сети подтвердил это «операционное» изменение сайту TechCrunch и объяснил, что новая политика будет распространяться как на Facebook, так и на Instagram.

Глава по глобальному управлению политикой компании Моника Бикерт (Monika Bickert) рассказала, что введение новых правил связано с выходом на британском телеканале Channel 4 документального фильма, в котором репортёр под прикрытием получил возможность поработать модератором Facebook. «С момента выхода программы мы работаем над обновлением руководства для модераторов, чтобы они блокировали все аккаунты, которые, скорее всего, принадлежат малолетним пользователям, даже если жалобы связаны с чем-то другим», – написала Бикерт.

***

24.07.2018

Facebook удаляет картины Брейгеля и Рубенса как нарушающие правила соцсети

Представители фламандского совета по туризму в шоке от цензуры в Фейсбук. Соцсеть удаляет картины знаменитых художников Рубенса, ван Эйка и Брейгеля из-за того, что на картинах изображены обнаженные тела, сообщает VRT (InternetUA).

Из-за столь странных ограничений бельгийские чиновники не могут рекламировать арт-выставки и другие события, посвященные изобразительному искусству.

Представители местного совета по туризму написали официальное письмо основателю Фейсбук Марку Цукербергу с просьбой пересмотреть политику его проекта.

«Дошло до смешного – цензура не пропустила картину Рубенса “Снятие с креста”. На это можно было бы закрыть глаза, если бы соцсеть не была столь популярной», – жалуются бельгийцы.

Отмечается, что ответа на жалобу чиновников пока нет.

***

25.07.2018

Twitter запретил регистрироваться под именем Илона Маска

Платформа Twitter начала блокировать все аккаунты, недавно поменявшие свое название на «Илон Маск». Об этом сообщает The Verge (InternetUA).

Эта мера была принята в рамках борьбы с мошенниками, которые пользуются именем миллиардера, который якобы раздает свои биткоины даром.

Такие аккаунты подписаны именем Маска и выглядят очень похожими на оригинальный профиль.

В случае если владелец аккаунта захочет некоторое время побыть Маском, его профиль в Twitter будет заблокирован, а на почту придет сообщение с просьбой подтвердить свою личность. После предоставления нужных данных профиль будет разблокирован.

***

1.08.2018
МІП і Фейсбук: поглиблення двосторонньої комунікації

Заступник Міністра інформаційної політики України Дмитро Золотухін провів зустріч з представниками компанії Фейсбук під час перебування з робочим візитом у Лондоні на запрошення Уряду Великої Британії...

Представники соціальної мережі вчергове запевнили Дмитра Золотухіна в тому, що в питаннях імплементації політик Фейсбуку немає жодного конфлікту інтересів, а саме – громадяни Росії не здійснюють модерації контенту, створюваного українськими користувачами, та не мають впливу на процес прийняття рішень щодо блокування та видалення контенту, який порушує стандарти спільноти.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

19.07.2018
Кабмин предлагает создать резервное хранилище госинформации

В Раде зарегистрирован проект закона Кабинета Министров № 8608 о внесении изменений в некоторые законы Украины, относительно решения вопроса сохранения резервных копий информации и сведений государственных электронных информационных ресурсов на случай кибератак (InternetUA).

«С целью выполнения мероприятий по нейтрализации факторов, которые могут привести к реализации угроз кибербезопасности... предусмотрено определить Государственную службу специальной связи и защиты информации Украины органом, ответственным за сохранение резервных копий информации и сведений государственных электронных информационных ресурсов, а также установление порядка передачи, хранения и доступа к этим копиям», – говорится в пояснительной записке к проекту закона.

«Одновременно, с целью устранения разночтения в терминологии, уже используется в действующем законодательстве, в понятийный аппарат законопроекта вводится новый термин “государственные электронные информационные ресурсы”. Целью законопроекта является законодательное

урегулирование возможности осуществления Государственной службой специальной связи и защиты информации Украины задач по сохранению резервных копий информации и сведений государственных электронных информационных ресурсов», – подчеркивают авторы документа.

***

21.07.2018

British Airways потребовала от клиентов публиковать личные данные в Twitter

Британский авиаперевозчик British Airways потребовал от своих клиентов публиковать в Twitter ряд персональных данных, включая номера паспортов, полные адреса и другую конфиденциальную информацию, мотивируя это тем, что сведения помогут разобраться в случае возникновения жалоб на обслуживание. Как поясняет компания, данное требование связано с соблюдением норм Общего регламента по защите данных (GDPR), вступившего в силу 25 мая нынешнего года (InternetUA).

Новый регламент призван предотвратить сбор и продажу компаниями персональной информации пользователей без их согласия, потому не совсем понятно, какими соображениями руководствуется British Airways, требуя публиковать личные данные в публичном доступе в соцсети.

По словам специалиста в области безопасности Мустафы Аль-Бассам (Mustafa Al-Bassam), обратившего внимание на ситуацию, после жалоб некоторых пользователей авиакомпания изменила формулировку и попросила отправлять информацию в личных сообщениях. Кроме того, Аль-Бассам обнаружил еще одну проблему. Как оказалось, British Airways использует трекеры при проверке клиентами данных о рейсе в браузере и отправляет сведения сторонним компаниям без согласия пользователей (на сайте перевозчика нет формы согласия или опции отказа), что является прямым нарушением требований GDPR.

***

23.07.2018

9 советов по повышению безопасности в Интернете

В Интернете буквально каждый день появляются новости о новых вирусах, о крупных взломах и хакерах. Тем не менее, большинство пользователей считает, что их это никогда не коснется. Возможно, это и так, но это не значит, что не нужно беспокоиться о своей безопасности.

Докладніше

***

23.07.2018

Специалисты раскрыли кибершпионов, заражающих компьютеры украинских госучреждений

Исследователи компании ESET обнаружили кибершпионскую кампанию, нацеленную на украинские госучреждения. Злоумышленники заражают компьютеры жертв вирусами Quasar RAT, Sobaken и Vermin со схожим исходным кодом, с помощью которых похищают данные и аудиозаписи разговоров с компьютеров жертв.

Докладніше

***

23.07.2018

Safari в iOS 12 научился определять хакерские действия на сайтах

Apple продолжает усиливать безопасность в своих устройствах. В iOS 12 компания реализовала новую интересную функцию (InternetUA).

Теперь браузер Safari отслеживает подозрительную деятельность на сайтах и сообщает, в случае чего, об этом пользователю. Лично я смог заметить это нововведение на сайте одного из онлайн-кинотеатров.

iOS-устройство будет оповещать пользователя о том, что веб-сайт может тайно считывать вашу клавиатуру, либо пытаться обманным способом заставить вас ввести личные данные. Включая данные кредитных карточек.

Тем самым, вы можете мгновенно выйти из полноэкранного режима просмотра ролика, а затем и резко закрыть сайт. Полезная фишка, однако.

***

23.07.2018

Хакеры пытаются создать ботнет из маршрутизаторов D-Link и Dasan

Компания eSentire Threat Intelligence сообщила о новой вредоносной кампании, нацеленной на уязвимые маршрутизаторы от производителей D-Link и Dasan. По словам специалистов, хакеры пытаются создать ботнет из уязвимых устройств (InternetUA).

Исследователи зафиксировали массовые попытки эксплуатации с более чем 3 тыс. различных IP-адресов. Атака была нацелена на модели D-Link 2750B и Dasan GPON, работающих под управлением прошивки GPON.

«Ботнеты, построенные с помощью скомпрометированных маршрутизаторов, могут в конечном итоге сдаваться в аренду другим хакерам, использующим их для вымогательств, DDoS-атак и других целей», – отметили специалисты.

Как сообщили эксперты, атака велась в течение 10 часов. Злоумышленники попытались проэксплуатировать уязвимость CVE-2018-

10562, присутствующую в маршрутизаторах с версией прошивки ZIND-GPON-25xx.

***

30.07.2018

Со всех государственных сайтов США требуют удалить Flash

По словам сенатора Рона Уайдена, он не хочет повторения «ситуации с Windows XP», поэтому призывает удалить весь Flash с сайтов госорганов за год до окончания официальной поддержки этой технологии.

Докладніше

***

30.07.2018

Хакеры атакуют пользователей с помощью нового набора эксплоитов

Исследователи безопасности из компании Trend Micro обнаружили новый набор эксплоитов Underminer, активно использующийся для кибератак в странах Азии (InternetUA).

По словам специалистов, данный набор существует уже несколько месяцев, однако его активное использование злоумышленниками было зафиксировано лишь недавно. Наибольшая доля атак с использованием Underminer приходится на Японию (70 %), Тайвань (10 %), Южную Корею (6 %) и пр.

Количество эксплоитов в наборе сравнительно небольшое. В частности, в нем присутствуют вредоносные программы для эксплуатации следующих уязвимостей:

CVE-2015-5119 – уязвимость использования после освобождения (use-after-free) в Adobe Flash Player (исправлена в июле 2015 года).

CVE-2016-0189 – уязвимость повреждения памяти в Internet Explorer (исправлена в мае 2016 года).

CVE-2018-4878 – использования после освобождения (use-after-free) в Adobe Flash Player (исправлена в феврале 2018 года).

Ни один из эксплоитов не является уникальным для Underminer, все они уже использовались в других наборах. В частности, один из инструментов предназначен для проникновения в систему через TCP-туннели, второй – для сохранения присутствия, а третий – для установки майнера криптовалют.

***

31.07.2018

Появился новый крипто-майнер, нацеленный на крупные компании

Специалисты Лаборатории Касперского обнаружили новый вид вредоносного программного обеспечения (ПО) для скрытого майнинга под названием PowerGhost, нацеленного на крупнейшие корпорации в разных странах (InternetUA).

Зловред умеет незаметно закрепляться в системе и распространяется внутри крупных корпоративных сетей, заражая как рабочие станции, так и сервера. Сообщается, что PowerGhost встречается в Индии, Бразилии, Колумбии и Турции. После того, как вредоносное ПО заражает компьютер, запускается процесс майнинга криптовалют.

По словам специалистов Лаборатории Касперского, рост популярности и стоимости криптовалют убедил киберпреступников в необходимости вкладывать ресурсы в разработку новых техник для майнеров, которые постепенно приходят на смену троянцам-вымогателям.

Вирус-майнер PowerGhost, который мы исследовали, указывает на то, что киберпреступники изменили целевую аудиторию: теперь под прицелом хакеров крупные предприятия, а не отдельные пользователи. Таким образом, майнинг криптовалют станет огромной угрозой для бизнес-сообщества.

***

31.07.2018

Пользователей WhatsApp атаковал «страшный» вирус

Пользователи WhatsApp столкнулись с появлением в списке контактов нового абонента под названием Momo. Неизвестный номер появляется безо всяких причин и отправляет пользователям новости и фотографии шокирующего содержания, пишет Bild.de (InternetUA).

Особенностью работы «страшного» бота является то, что сообщения от него зачастую приходят в три часа ночи. Кроме того, робот может и позвонить пользователю по видеосвязи – при этом на экране появится зловещее изображение существа, похожего на девушку-ворону.

По данным Bild, «Момо» – это название скульптуры, представленной в Японии в 2016 году. Она имеет такое же необычное лицо и когтистые ноги-лапы. Специалисты полагают, что бот является шуткой авторства неизвестных хакеров.

Отмечается, что с 11 июля оригинальный номер «Момо», зарегистрированный в Японии, не выходил в онлайн, однако не исключается появление клонов злонамеренного бота. Его жертвами стали пользователи стран Испании Мексики и ряда других сран. Не исключено, впрочем, что все происходящее – подготовка к анонсу нового фильма-ужастика.

***

31.07.2018

На Прикарпатті поліція оголосила підозру хакеру у розповсюдженні шкідливого програмного забезпечення

Створений молодиком вірус призначався для отримання зловмисниками несанкціонованого віддаленого доступу до враженого пристрою (InternetUA). Наразі за фактом розповсюдження шкідливого програмного забезпечення триває досудове розслідування.

Працівники Карпатського управління Департаменту кіберполіції в Івано-Франківській області, за процесуального керівництва прокуратури міста Івано-Франківськ, викрили 21-річного жителя Калущини у створенні та розповсюдженні в мережі Інтернет шкідливого програмного забезпечення.

За даним фактом поліція розпочала кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України.

Оперативники з кіберполіції встановили, що шкідливе програмне забезпечення чоловік замаскував під програми чіт-кодів до комп'ютерних ігор. В подальшому, зловмисник завантажив у вільному доступі архівні файли на сайт файлообмінника, звідки користувачами сайту і завантажувалося ШПЗ.

За місцем проживання зловмисника поліцейські провели санкціонований обшук. Відтак, вилучено комп'ютерну техніку, яку вподальшому було направлено на експертне дослідження. За його результатами експерти виявили на комп'ютері зловмисника вірус, який він поширював у мережі.

На підставі зібраних доказів мешканцю Прикарпаття оголошено про підозру за вчинення злочину передбаченого ч. 1 ст. 361-1 Кримінального кодексу України. Слідство триває.

***

1.08.2018

Злоумышленники взломали более 10 тыс. сайтов на WordPress для распространения вредоносной рекламы

Исследователи безопасности из компании Check Point, обнаружили новую кампанию по распространению вредоносной рекламы, в ходе которой заражается порядка 40 тыс. устройств каждую неделю.

Докладніше

***

1.08.2018

США обвинили в совершении кибератак трех граждан Украины

США обвинили трех граждан Украины в совершении кибератак. Об этом сообщается на сайте Министерства юстиции США (InternetUA).

Согласно сообщению ведомства, граждане Украины Дмитрий Федоров, Федор Хладыр и Андрей Колпаков являются членами хакерской группы,

широко известной как «FIN7» (также называемой «Carbanak Group» и «Navigator Group»).

По версии следствия, с, как минимум, 2015 года члены «FIN7» занимались рекламной кампанией, нацеленной на более чем 100 компаний в США, преимущественно в ресторанной, игровой и гостиничной индустриях. Как указано в обвинительных заключениях, члены «FIN7» взломали тысячи компьютеров и украли миллионы данных кредитных и дебетовых карт клиентов компаний, которые впоследствии «FIN7» использовала в своих целях или продавала.

«Поскольку хакеры стремятся найти новые способы нанесения вреда американской общественности и нашей экономике, Министерство юстиции по-прежнему готово к сотрудничеству с нашими партнерами по обеспечению соблюдения законов, чтобы выявлять, пресекать и преследовать виновных в этих угрозах», – сказал помощник генерального прокурора США Брайан Бенчковски.

Минюст США также отметил, что «только в США "FIN7" смогла успешно проникнуть в компьютерные сети компаний в 47 штатах и округа Колумбии, и украсть более 15 миллионов данных кредитных карт клиентов».

***

1.08.2018

Facebook отключает доступ к данным пользователей сотням тысяч приложений

Соцсеть Facebook накануне объявила об отключении доступа к своему программному интерфейсу (API) для разработчиков сотен тысяч неактивных приложений. Таким образом, разработчики лишились доступа к данным пользователей соцсети, утечки которых стали поводом для нескольких скандалов (InternetUA).

Как пишет The Verge, Facebook объявила о намерении отключить доступ к API 1 августа на майской конференции для разработчиков. Чтобы избежать этого, разработчикам приложений необходимо было подтвердить активность приложений и заключить новые контракты, касающиеся сбора данных пользователей соцсети.

Цель этого шага Facebook состоит в том, чтобы убедиться, что партнеры компании отвечают ее обновленным требованиям в области защиты данных, которые вступили в силу после того, как СМИ сообщили об утечке данных миллионов пользователей одного из приложений. Затем эти данные использовались компанией Cambridge Analytica во время избирательной кампании Дональда Трампа.

В компании порекомендовали всем приложениям, которые еще используются, пройти процедуру проверки, которая не займет много времени. Если в ходе проверки у Facebook возникнут дополнительные вопросы,

разработчикам необходимо будет оперативно предоставить нужную информацию, иначе приложение будет лишено доступа к API Facebook.

***

2.08.2018
Ирина Фоменко
Хакеры подсоединили парковочный терминал к порносайту

Хакеры подсоединили парковочный IoT-терминал к порносайту, что, как предполагается, было атакой без злого умысла со стороны «серой шляпы».
Докладніше

***

2.08.2018
Исследование: Telegram Passport уязвим брутфорс атакам

Разработчик криптографического ПО Virgil Security, сообщает, что недавно выпущенный инструмент для идентификации личности Telegram Passport оказался уязвим для брутфорс атаки.
Докладніше

ДОДАТКИ

Додаток 1

23.07.2018
Facebook, Google, Microsoft и Twitter объединятся для удобства пользователей

20 июля 2018 года в блоге Google была опубликована заметка, согласно которой ведущие компании объединят усилия, чтобы пользователям было проще загружать изображения с одного ресурса на другой (IGate).

Согласно сообщениям Google, подобный проект возник еще в 2007 году. Тогда над его воплощением трудилась небольшая группа инженеров. В 2011 году корпорация запустила сервис Takeout, при помощи которого пользователи могли сохранять копии сохраненных данных в различных форматах. Теперь этот сервис трансформируется в Data Transfer Project с открытым кодом.

«Data Transfer Project – это инициатива по создания сервиса с открытым кодом, призванная привлечь в свои ряды как можно больше сервисов. Он расширит возможности для переноса данных за счет снижения нагрузки на инфраструктуру как для провайдеров, так и для пользователей, что в свою очередь приведет к появлению новых услуг. Протоколы и методология Data Transfer Project позволяют осуществлять передачу данных как от сервиса к сервису, так и напрямую к пользователю», – говорится в описании проекта.

Инициативу уже поддержали Facebook, Microsoft и Twitter. Это значит, что переносить фото, опубликованные на одном из этих ресурсов, на другой станет гораздо проще. Пользователи также смогут применять одну учетную запись для авторизации на различных сервисах, делиться необходимым контентом и переносить избранные медиатеки автоматически.

На данный момент компании обсуждают, как именно будет работать проект. Для широкого круга подписчиков эта инициатива станет доступна еще не скоро.

(вгору)

Додаток 2

24.07.2018

Девять скрытых функций Instagram, о которых вы могли не знать

Даже если вы установили Instagram на свой телефон, вы, вероятно, не знаете все, на что он способен. В данной статье я расскажу вам о десяти скрытых функциях приложения, которые вы можете использовать как на Android, так и на iOS (InternetUA).

Изменяйте фильтры

Изначально основной особенностью Instagram были фильтры, которые накладывались на фотографию и делали ее более яркой. Сегодня фильтры по-прежнему являются основным набором инструментов, который вы видите после того, как добавите фото в приложение. Возможно, вы не знаете, что после выбора фильтра вы можете изменить его силу, чтобы получить более подходящий эффект.

Чтобы определить, каким будет изменение, выберите фильтр, а затем снова нажмите на его миниатюру. Должен появиться слайдер: используйте его для настройки силы фильтра, а затем нажмите «Готово».

Вот еще один быстрый совет, позволяющий скрыть фильтры, которые вы часто не используете: прокрутите до конца списка фильтров и нажмите «Настройки», чтобы добавлять или удалять фильтры, которые вам нравятся или не нравятся.

Получайте уведомления от ваших любимых людей

Мы все боремся с большим количеством уведомлений, которые приходят на наши смартфоны. К счастью, в Instagram вы можете их настроить, чтобы видеть оповещения только от близких людей в том случае, когда они опубликуют что-то новое. Этот параметр работает только для пользователей, которые подписаны на вас, и он также довольно хорошо скрыт внутри приложения.

Во-первых, вам нужно перейти на страницу профиля соответствующего человека внутри Instagram. Нажмите три точки в правом верхнем углу, затем выберите «Включить уведомления о публикациях», чтобы получать уведомления о новых постах, или «Включить уведомления об историях», чтобы сразу видеть новые сторис своего друга.

Рассматривайте мир

Конечно, вы любите своих друзей и семью, но они не всегда публикуют интересные фотографии. Нажмите на вкладку «Поиск» (значок увеличительного стекла), чтобы просмотреть общедоступные фотографии и видеоролики пользователей по всему миру.

Одним из полезных способов использования вкладки «Поиск» является проверка различных мест (городов, достопримечательностей, ресторанов, музеев) перед их посещением. Просто введите название города или место в поле поиска в верхней части экрана, перейдите на вкладку «Места» и выберите правильный результат. Вы увидите множество фото и видео.

Сохраняйте фотографии для последующего просмотра

Недавно в Instagram добавили возможность оставлять закладки на фотографии, которые вам нравятся, чтобы вы могли посмотреть их позже. Никто кроме вас не сможет увидеть записи и коллекции, которые вы сохранили, даже учетную запись, с которой вы сохраняете фотографии.

Чтобы сохранить любую фотографию или видео, нажмите один раз на значок закладки – он выглядит как хвост ленты. Или нажмите и удерживайте этот значок, чтобы поместить пост в определенную коллекцию. Если вы хотите просмотреть все сохраненные посты, откройте приложение, перейдите на вкладку «Профиль» и нажмите значок закладки.

Используйте приложение для обмена мгновенными сообщениями

За последние семь лет Instagram прошел долгий путь, добавив в свой список все больше возможностей. И одна из этих функций – обмен мгновенными сообщениями. Они не должны обязательно включать фотографию, это может быть обычный текст.

Если вы нажмете на значок «Отправить» в правом верхнем углу экрана, вы сможете написать сообщение любому человеку из списка ваших контактов. Если же вы хотите отправить сообщение нескольким контактам, вам повезло, Instagram также поддерживает групповые чаты.

Сделайте свои «Истории» более приватными

Instagram не постеснялась перенять лучшие возможности Snapchat. Например, недавно они добавили возможность создания «Историй» (Stories) – фотографии и видеоролики пользователей, которые появляются в верхней части экрана в течение 24 часов, прежде чем исчезнуть. Но прежде чем вы разместите такую «Историю», вы можете выбрать, кто сможет видеть эти временные сообщения.

«Истории» не отображаются в вашем профиле Instagram, и вы можете не хотеть, чтобы они были такими же общедоступными, как ваш основной канал. Для этого откройте свой профиль, перейдите на страницу параметров Instagram и выберите «Настройки истории». Здесь вы можете скрывать свои «Истории» от определенных контактов.

Сохраняйте исходные файлы

Когда вы размещаете в Instagram одну из ваших фотографий, приложение изменяет ее размер с целью сократить размер данных и время загрузки, а также,

чтобы другие не могли сохранить ваши изображения в их полном разрешении. Но что, если вы хотите сохранить полноразмерные копии? Вы можете сохранить их отдельно.

Перейдите на страницу своего профиля и нажмите верхнюю правую кнопку (три точки), чтобы перейти к экрану настроек Instagram. Затем прокрутите вниз и найдите меню «Исходные фото». Здесь вы можете разрешить сохранять исходные фотографии на ваше устройство.

Делитесь своими фотографиями везде

Instagram содержит некоторые полезные параметры для обмена фотографиями в других социальных сетях, чтобы все ваши друзья могли их видеть.

На последнем шаге перед публикаций фотографии в Instagram вы можете выбрать одну или несколько социальных сетей, таких как «ВКонтакте», Facebook, Twitter или Tumblr, чтобы поделиться своим постом в них. Для еще большего количества опций используйте бесплатную услугу IFTTT или If This Then That. Вы можете не только делиться своими сообщениями Instagram с другими платформами, но также делать больше с вашими фотографиями и видео, например, автоматическую резервную копию ваших фото на Dropbox или Google Drive.

Посмотрите, что делают ваши друзья

В Instagram есть специальная вкладка «Активность» (символ сердца), которая так же как и «Лента новостей в Facebook» дает удобный способ проверить, что делают ваши друзья, а также найти новых интересных людей.

Нажмите значок сердца в нижней части экрана, затем вкладку «Подписки» вверху, и вы получите отредактированный обзор того, что происходило в вашей сети Instagram. Нажмите на любую фотографию, видео или пользователя для получения более подробной информации. Чтобы увидеть свою деятельность, нажмите вкладку «Вы».

(вгору)

Додаток 3

26.07.2018

МІП: Через Facebook діти можуть звернутися на «гарячу» лінію за допомогою

26 липня 2018 року в ІА «Укрінформ» відбувся круглий стіл «Безпека дитини в Інтернеті», організований Міністерством інформаційної політики України спільно з ГО «Ла Страда Україна». Учасники дискусії обговорили, які сучасні загрози чекають на дітей в Інтернеті, як убезпечити від них юних користувачів і куди можна звернутися за допомогою в мережі (Міністерство інформаційної політики).

Заступник Міністра інформаційної політики України Дмитро Золотухін зазначив, що буденне використання Інтернету дітьми приховує в собі ризики, про які дорослі користувачі можуть і не здогадуватися. «Оскільки сучасні діти

отримують до рук телефон раніше, ніж починають говорити, перед усіма нами гостро постає проблема їхньої безпеки в мережі. Молодші юзери потребують розвинутого критичного мислення, обізнаності та розуміння віртуального світу, які ми зобов'язані їм дати, щоб захистити від можливих негативних впливів. Більше того, наша задача – створити для дітей механізми звернення за допомогою в разі необхідності. Це можливо лише за співпраці уряду, громадського суспільства та світових корпорацій».

Президентка громадської організації «Ла Страда Україна» Ольга Калашник розповіла, куди можна звертатися за допомогою в мережі: «Міністерство інформаційної політики ініціювало партнерство «Ла Страда Україна» з офісом Facebook. Як наслідок цього, телефони Національної «гарячої» лінії розміщені в розділі «Центр безпеки Фейсбук». Тож у небезпечних ситуаціях українські користувачі, зокрема діти, можуть знайти ці контакти та звернутися за консультацією чи порадою. Приклади співпраці громадянського суспільства, центральних органів виконавчої влади та провідних соціальних мереж мають поширюватись і наслідуватись».

Керівник відділу нових медіа ГО «Інтерньюз Україна» Віталій Мороз переконаний, що діти іноді краще розуміють технології, аніж дорослі, але у свою чергу їм властиві додаткові ризики. «Загрози в онлайн-просторі та в сфері цифрової безпеки для дітей варто розглядати в ширшому контексті швидких технологічних змін в суспільстві та загальної вразливості користувачів, яким переважно не властиві превентивні кроки щодо убезпечення себе в Інтернеті», – зауважив Мороз.

Журналістка Інтернет-видання MediaSapiens ГО «Детектор медіа» Катерина Толокольнікова розповіла: «Для дітей цілком конкретними небезпеками є шахрайство з даними та грошима, або ж знайомства зі злочинцями, які можуть завдати шкоди в реальному житті. Проте, перебування онлайн також чинить значний вплив на психічне здоров'я підлітків. Мова йде не лише про травматичний досвід від перегляду контенту з насильством чи залежність від гаджетів, а й про погіршення навичок спілкування та цькування, яке може призвести до депресій, а часом і самогубств». Допомогти ж підліткам зорієнтуватися у світі медіа та Інтернету, зокрема навчити, як захистити себе в мережі, може мультимедійний онлайн-посібник з медіаграмотності для підлітків «МедіаДрайвер» , розроблений ГО «Детектор медіа».

Надія Дятел, співробітниця Лабораторії психології масової комунікації та медіаосвіти Інституту соціальної та політичної психології НАПНУ, підтвердила, що однією із загроз, з якими зустрічались в Інтернеті підлітки, є кібербулінг. Про це, за її словами, говорять результати всеукраїнського експерименту, що проводився Лабораторією психології масової комунікації та медіаосвіти.

У свою чергу, Олена Черних, голова Правління Центру кращого Інтернету та координаторка Національного комітету Дня безпечного Інтернету в Україні, запросила до відзначання Дня безпечного Інтернету 2019, який відбудеться 5 лютого. «В Україні цей день є одним із ключових для поширення

ідей безпечного користування Інтернетом та сучасними цифровими технологіями. Тому ми вже розпочали підготовку, зокрема, Центр кращого Інтернету працює над аналізом нових рекомендацій Ради Європи із захисту дитини в цифровому просторі задля сприяння імплементації їх основних положень у нашій країні», - пояснила Черних.

Участь в обговоренні також взяли представники Управління ювенальної превенції Національної поліції України, Кіберполіції України, мобільного оператора lifecell, мНУО «Європейська медіа платформа».

Нагадаємо, що з 24 листопада 2017 року за номером 116 123 (доступний з мобільних телефонів на всій території України) розпочала роботу «гаряча» лінія з попередження домашнього насильства, торгівлі людьми та ґендерної дискримінації, роботу якої забезпечує ГО «Ла Страда-Україна».

(вгору)

Додаток 4

22.07.2018

Facebook прекратил сотрудничество с фирмой, которая могла передавать данные властям

Facebook приостановила сотрудничество с американской фирмой, которая имела контракты с правительством США и другими странами, и изучает случаи возможного нарушения ею правил соцсети, касающихся передачи данных пользователей третьей стороне (InternetUA).

По данным The Wall Street Journal, речь идет о базирующейся в Бостоне (штат Массачусетс) фирме Crimson Hexagon, у которой в последние годы было заключено множество контрактов на анализ публичных данных пользователей Facebook.

Как утверждает издание, среди клиентов фирмы были, в частности, несколько правительственных ведомств США, Турции, а также российская некоммерческая организация Фонд развития гражданского общества, специализирующаяся на исследованиях в области политики. По версии газеты, последняя якобы связана с властями России и с помощью баз данных Crimson Hexagon изучала общественное мнение граждан РФ по поводу ситуации в стране.

Как отмечает издание, Facebook практически не контролировала то, как бостонская фирма использует данные, собранные ею в соцсети. Многие правительственные контракты с Crimson Hexagon не были заранее одобрены Facebook. Соцсеть заблокировала приложение фирмы в Facebook и Instagram и начала расследование на предмет неправомерного использования личной информации пользователей, отмечается в материале.

Главой и основателем Crimson Hexagon является профессор Гарвардского университета Гэри Кинг, который сотрудничает с руководством Facebook. Он также является главой проекта Social Science One, который разрабатывается вместе с Facebook.

В его рамках социальная сеть намеревалась предоставить исследователям доступ к обширным массивам анонимных данных Facebook для оценки того, какое влияние соцсеть оказывает на электоральные процессы. Изучению подлежат, в частности, данные, касающиеся ссылок, которые задействовали пользователи соцсети, в том числе те, которые вели на заведомо ложные новостные публикации.

Поводом для проведения исследований стал скандал, разразившийся после материала газеты The New York Times о передаче данных соцсети ныне уже не действующей британской компании Cambridge Analytica. По разным оценкам, речь шла о персональных данных примерно 87 млн пользователей.

Главе Facebook Марку Цукербергу в апреле пришлось в связи с этим выступить на двух слушаниях в Конгрессе США. Он заверил законодателей, что впредь в соцсети будут бережнее обращаться с личными данными пользователей.

(вгору)

Додаток 5

28.07.2018

Борьба с нарушителями привела к падению аудитории Twitter

Twitter опубликовал отчёт по итогам второго квартала, завершившегося 30 июня 2018 года (IGate).

Выручка выросла на 24 % год к году и составила $711 млн. 84,5 % ($601 млн) выручки пришлось на рекламу.

Чистая прибыль составила $100 млн против убытка $116 млн годом ранее. Twitter показывает прибыль последние девять месяцев, а второй квартал 2018 года стал рекордным, отмечает Reuters.

Дневная аудитория Twitter выросла на 11 %, абсолютные показатели в отчётности не раскрываются. В отличие от месячной аудитории, в дневной компания считает только тех пользователей, которые пользуются официальными приложениями Twitter и веб-версией сервиса.

Месячная аудитория сервиса составила 335 млн активных пользователей. По сравнению со вторым кварталом 2017 года аудитория выросла на 9 млн, но по сравнению с первым кварталом 2018 года сократилась на 1 млн.

Сокращение месячной аудитории в Twitter связали с новыми правилами защиты данных пользователей Евросоюза (GDPR) и зачисткой платформы от «токсичных» пользователей, которые оскорбляют остальных и распространяют фальшивые новости.

Twitter удалил около 70 млн учётных записей в мае и июне, но большинство из них не войдут в отчёт, так как неактивны на платформе в течение 30 дней и больше, говорил в начале июля финансовый директор компании Нед Сигал.

Кроме этого, Twitter решил прекратить сотрудничество с SMS-операторами некоторых стран, отказавшись платить за возможность

пользователей публиковать твиты с помощью SMS. В компании уверенны, что смогут обеспечить лучший пользовательский опыт с помощью приложений Twitter и Twitter Lite.

В Twitter ожидают, что в третьем квартале снижение месячной аудитории продолжится, но будет находиться в пределах единиц миллионов, что предполагает последовательное снижение примерно до 330 млн пользователей, указывает Twitter.

После публикации отчётности акции Twitter на предварительных торгах упали на 18 %, позднее падение скорректировалось до 12-13 %. На открытии Нью-Йоркской фондовой биржи акции Twitter упали на 13 %. Капитализация компании снизилась с $32 млрд до $28 млрд.

(вгору)

Додаток 6

1.08.2018
МІП і Фейсбук: поглиблення двосторонньої комунікації

Заступник Міністра інформаційної політики України Дмитро Золотухін провів зустріч з представниками компанії Фейсбук під час перебування з робочим візитом у Лондоні на запрошення Уряду Великої Британії (Міністерство інформаційної політики).

Провідна фахівчиня компанії з питань політики соціальної мережі у сфері контртероризму Д-р Ерін Марі Салтман, Керівник напрямку Політики Фейсбуку в Центральній та Східній Європі Габріела Чех та заступник Міністра обговорили процес вдосконалення політик Фейсбуку та їх імплементації.

Представники соціальної мережі вчергове запевнили Дмитра Золотухіна в тому, що в питаннях імплементації політик Фейсбуку немає жодного конфлікту інтересів, а саме – громадяни Росії не здійснюють модерації контенту, створюваного українськими користувачами, та не мають впливу на процес прийняття рішень щодо блокування та видалення контенту, який порушує стандарти спільноти.

Разом з тим, представники компанії запевнили, що Фейсбук продовжує працювати над вдосконаленням політик та їх імплементації. Так, зокрема, будуть розширені можливості більш ретельного та докладного пояснення користувачам суті порушень стандартів спільноти, які вони вчинили, а також буде вдосконалюватися можливість оскаржувати рішення про блокування контенту користувачів.

Дмитро Золотухін, у свою чергу, ознайомив представників компанії з ситуаціями, які викликають глибоке занепокоєння з боку Міністерства інформаційної політики України, щодо можливих порушень свободи слова внаслідок блокування українських журналістів і блогерів.

Сторони досягли домовленості підтримувати обмін інформацією стосовно конкретних ситуацій з блокуванням українських користувачів, за умов наявності детальних відомостей щодо причин та обставин блокувань.

Представники Міністерства зможуть за необхідності направляти деталізовану інформацію про блокування українських користувачів для додаткового розгляду на предмет наявності фактів порушення стандартів спільноти Фейсбук.

Окрім зазначеного, Дмитро Золотухін також довів до відома представників компанії Фейсбук юридичну позицію України щодо фактів терористичної діяльності представників так званих ДНР і ЛНР, а також фінансової та іншої підтримки цієї терористичної діяльності з боку Російської Федерації. Пані Ерін Марі Салтман підкреслила, що компанія Фейсбук дуже уважно ставиться до проблем протидії тероризму та здійснює масштабну діяльність щодо протидії проявам інформаційної підтримки насильства чи насильницької ідеології.

(вгору)

Додаток 7

23.07.2018

9 советов по повышению безопасности в Интернете

В Интернете буквально каждый день появляются новости о новых вирусах, о крупных взломах и беснующихся хакерах. Тем не менее, большинство пользователей считает, что их это никогда не коснется. Возможно, это и так, но это не значит, что не нужно беспокоиться о своей безопасности (InternetUA).

Рассказываем, как можно защитить себя и личную конфиденциальную информацию в Интернете.

В первую очередь необходимо проверить настройки приватности в соцсетях

Социальные сети собирают огромное количество информации о людях, которые их используют. Многих может по-настоящему шокировать количество персональных данных, находящихся в свободном доступе. Частично справиться с этой проблемой можно, изменив настройки приватности в соцсетях. Если открыть параметры того же Instagram или Facebook, то в них найдется с десяток пунктов, позволяющих ограничить доступ посторонних лиц к той или иной информации.

Не стоит использовать публичные облачные сервисы для хранения персональных данных

Случайно выдать какую-то важную информацию можно не только в соцсетях, но и в облачных сервисах, которые, на первый взгляд, кажутся безопасными. Люди используют публичные сервисы вроде Google Docs для хранения там баз данных, паролей, отсканированных документов и так далее. Безусловно, так делать нельзя. Сервисы, созданные для совместной работы, не подходят для хранения конфиденциальной информации. Лучше использовать более узкоспециализированные продукты. Например, 1Password.

Нужно всячески избегать рекламный трекинг в сети

Больше остальных добраться до пользовательских данных хотят рекламисты. Маркетологи используют любые крупицы информации о человеке, чтобы создать специальный профиль, на который смогут ориентироваться рекламодатели, чтобы максимально эффективно воздействовать на человека. К счастью, пользователям macOS и iOS не нужно беспокоиться по поводу трекинга. На протяжении нескольких лет корпорация работает над тем, чтобы если не устранить трекинг, то хотя бы ограничить его до минимума.

По возможности стоит скрывать свои основные почтовый адрес и номер телефона

Чтобы не нарваться на спам, необходимо использовать свой почтовый ящик и телефон только на доверенных сайтах. Для регистрации на сомнительных ресурсах стоит использовать второстепенные данные. Или вовсе завести одноразовый e-mail, чтобы в случае чего не обнаружить потом в почтовом ящике десятки писем от всевозможных магазинов.

Следует использовать мессенджеры с оконечным шифрованием

Сейчас почти все современные мессенджеры оснащены продвинутыми системами шифрования данных. Из-за этого даже возникают скандалы государственных масштабов. Взломать такие мессенджеры извне просто невозможно. Поэтому их и ценят за сохранение приватности. К таким мессенджерам относятся, например, WhatsApp, iMessage и секретные чаты в Telegram.

Пароли должны быть сложными и разными

Сейчас о безопасности паролей говорят везде. Сложные 12-символьные пароли превратились в культ и жизненную необходимость. И подобное средство защиты трудно переоценить. Это не паранойя, а реальная возможности спасти свои данные. Только вот запомнить такие пароли чрезвычайно сложно. А ведь еще нужно создавать новый для каждого сервиса. На помощь приходят современные браузеры и программы для хранения паролей. Те, кто используют Safari знают, что фирменный браузер Apple сам создает пароли и хранит их в облаке, чтобы владельцу устройства больше никогда не пришлось их подбирать, придумывать и вспоминать. Естественно, пренебрегать этой функцией ни в коем случае нельзя.

Нельзя оставлять смартфон или компьютер без блокировки

Огромное количество людей никак не защищают свои компьютеры, планшеты и смартфоны. Просто оставляют их без пароля, без блокировки сканером отпечатков пальцев и так далее. Удивительно, но многим просто лень использовать подобные механизмы. Ведь Face ID или Touch ID могут не сработать. Тогда придется вводить код, а это долго муторно, да и вообще, его еще и запомнить надо. При этом многие руководствуются тем, что даже если и украдут смартфон, что они интересного там найдут. На самом деле много всего. Фотография, геопозиция, номера, почтовые адреса и еще много всего, что попав в не те руки, может разрушить жизнь. Поэтому всегда нужно ставить пароли и активировать Face ID с Touch ID и аналогами.

В целях соблюдения приватности можно скрыть уведомления на экране блокировки

Такая опция включена в iPhone X по умолчанию. Пока хозяин смартфона не посмотрит на экран, уведомления будут скрыты. То же самое можно сделать и на старых моделях смартфона Apple.

Для этого нужно:

– Открыть настройки устройства.

– Перейти в меню «Уведомления».

– Открыть подменю «Показ миниатюр» и выбрать пункт «Без блокировки».

После этого все уведомления будут скрываться, пока владелец смартфона или планшета не разблокирует его.

Следует избегать незащищенных публичных Wi-Fi-сетей

Публичные Wi-Fi-сети, пожалуй, одно из самых неудачных мест для проведения онлайн-транзакций или отправки каких-то важных данных. Эти сети обычно никак не защищены, а значит в трафик, который через них проходит, могут вмешаться посторонние люди. Они, в свою очередь, делают это, чтобы выудить какие-нибудь ценные сведенья, на которых потом можно заработать. По возможности стоит избегать такие сети. А если пришлось воспользоваться, то нужно заранее вооружиться хорошим VPN-сервисом.

(вгору)

Додаток 8

23.07.2018

Специалисты раскрыли кибершпионов, заражающих компьютеры украинских госучреждений

Исследователи компании ESET обнаружили кибершпионскую кампанию, нацеленную на украинские госучреждения. Злоумышленники заражают компьютеры жертв вирусами Quasar RAT, Sobaken и Vermin со схожим исходным кодом, с помощью которых похищают данные и аудиозаписи разговоров с компьютеров жертв (IGate).

Вирусы распространяются посредством фишинговых писем и уже заразили компьютерные сети нескольких сотен жертв из различных госучреждений Украины.

Quasar представляет собой вредоносное ПО с открытым исходным кодом, предназначенное для слежки и хищения данных из зараженной системы. Sobaken – модифицированная версия Quasar, в которой отсутствуют некоторые функции, но исполняемый файл меньшего размера, поэтому его легче скрыть.

Vermin – самый опасный из трех вредоносов. Помимо выполнения стандартных задач, таких как мониторинг происходящего на экране, загрузка файлов, он также содержит набор функций, которые позволяют включать запись звука, похищать пароли и считывать нажатия клавиш.

Примечательно, что вирусы модифицированы таким образом, чтобы работать только при русской или украинской раскладке с IP-адресами в пределах России или Украины. Если эти условия не соблюдены, вирус самостоятельно удалится.

Специалисты отмечают, что кампания активна по меньшей мере с октября 2015 года. В ESET за активностью хакеров наблюдают с середины 2017 года, а в январе 2018-го о кампании впервые сообщили публично, однако с тех пор ее масштабы только прогрессируют.

Кто стоит за атаками, пока неизвестно: атакующие, не обладая серьезными навыками и не имея доступ к неизвестным уязвимостям нулевого дня, мастерски используют социальную инженерию для незаметного распространения вирусов. «Это подчеркивает необходимость обучения персонала навыкам кибербезопасности, помимо наличия качественного решения в области безопасности», – подводят итог аналитики.

(вгору)

Додаток 9

30.07.2018

Со всех государственных сайтов США требуют удалить Flash

По словам сенатора Рона Уайдена, он не хочет повторения «ситуации с Windows XP», поэтому призывает удалить весь Flash с сайтов госорганов за год до окончания официальной поддержки этой технологии (InternetUA).

Долой Flash

Сенатор от штата Орегон Рон Уайден (Ron Wyden) выпустил открытое письмо, в котором призвал государственные учреждения США скорейшим образом отказаться от использования Adobe Flash на их сайтах.

Компания Adobe объявила, что свернет техническую поддержку Flash к концу 2020 г. Уайден призвал устранить все Flash-элементы на государственных сайтах к 1 августа 2019 г., чтобы избежать повторения ситуации с Windows XP.

Напомним, Microsoft официально прекратила поддержку своей операционной системы 2001 г. в 2014 г. после долгих проволочек. Windows XP оказалась настолько популярна и настолько глубоко интегрированна в крупных корпорациях и правительственных сайтах США, что некоторые из них до сих пор продолжают использовать ее, выплачивая Microsoft крупные суммы за сохранение технической поддержки.

«Федеральному правительству слишком часто не удавалось в надлежащий срок избавиться от устаревшего программного обеспечения», – указывает Уайден в своем письме, отмечая заодно, что у Flash имеются «серьезные, в основном не поддающиеся исправлениям проблемы с кибербезопасностью». По мнению сенатора, именно эти проблемы являются причиной, по которой правительственные учреждения должны полностью

отказаться от Flash еще до официального окончания его поддержки разработчиком.

Устаревшая и небезопасная технология

Уайден предлагает запустить пилотную программу, в рамках которой до 1 марта 2019 г. произошла бы частичная замена решений на базе Flash на более безопасные аналоги, а к 1 августа 2019 г. он был бы удален со всех правительственных компьютеров.

Письмо сенатора было направлено руководителям Национального института стандартов и технологий США, Агентства национальной безопасности и Министерству внутренней безопасности США.

«Мнение сенатора относительно Flash обосновано: эта технология действительно устарела, а ее уровень защищенности оказался недостаточно высоким, – в течение нескольких лет Flash являлся одним из главных источников киберугроз, – полагает Роман Гинятуллин, эксперт по информационной безопасности компании SEC Consult Services. – На сегодняшний день Flash – уходящая натура. Однако госорганы во всем мире обычно не торопятся производить замену оборудования или ПО, поэтому вероятность их полного отказа от Flash даже к 2020 году, к сожалению, невелика».

По данным W3Techs, сегодня менее чем 5 % от общего числа веб-сайтов в мире – будь то глобально популярные ресурсы или заброшенные частные страницы – все еще используют Flash в том или ином виде. К 2020 г. процент пользователей этой технологии, скорее всего, снизится до значений статистической погрешности.

(вгору)

Додаток 10

1.08.2018

Злоумышленники взломали более 10 тыс. сайтов на WordPress для распространения вредоносной рекламы

Исследователи безопасности из компании Check Point, обнаружили новую кампанию по распространению вредоносной рекламы, в ходе которой заражается порядка 40 тыс. устройств каждую неделю (InternetUA).

Как полагают специалисты, операторы данной кампании объединились с рекламной сетью и реселлерами для перенаправления жертв на мошеннические сайты, распространяющие вымогательское ПО, банковские трояны и другие вредоносы. Данная схема получила название Master134 по аналогии с адресом главного C&C-сервера кампании.

Согласно докладу, изначально мошенники взламывают сайты WordPress. Исследователи обнаружили более 10 тыс. сайтов, скомпрометированных в ходе данной кампании. На всех взломанных сайтах работает система управления контентом WordPress версии 4.7.1, в которой существует критическая уязвимость, позволяющая злоумышленникам удаленно выполнить код.

Взломав сайт, атакующие размещают на нем рекламные объявления, перенаправляющие пользователей на портал Master134.

Роль сервиса Master134 заключалась в том, чтобы продвигать рекламные места в рекламной сети AdsTerra под учетной записью издателя. Данные рекламные места затем скупались злоумышленниками для перенаправления жертв на вредоносные ресурсы.

По словам исследователей, почти все рекламные места покупались через реселлера AdsTerra. В числе покупателей значатся операторы наборов эксплоитов (RIG, Magnitude, GrandSoft, FakeFlash), систем распределения трафика (Fobos, HookAds, Seamless, BowMan, TorchLie, BlackTDS, Slyip) и мошеннических сайтов, маскирующихся под техподдержку.

«Похоже, что сотрудничество между различными группами злоумышленников успешно поддерживается через сторонние рекламные сети, самой крупной из которых является AdsTerra», – отметили специалисты.

«Основываясь на наших выводах, мы предполагаем, что злоумышленники платят Master134 напрямую. Master134 затем платит рекламной сети, чтобы перенаправить трафик и, возможно, даже скрыть его происхождение», – добавили они.

(вгору)

Додаток 11

2.08.2018
Ирина Фоменко
Хакеры подсоединили парковочный терминал к порносайту

Хакеры подсоединили парковочный IoT-терминал к порносайту, что, как предполагается, было атакой без злого умысла со стороны «серой шляпы». Об этом сообщает IoT News (InternetUA).

Наиболее известными названиями для хакеров являются «черные шляпы» или «белые шляпы» – они указывают, намерены ли хакеры нанести ущерб, или же они хотят найти уязвимости для защиты системы от компрометации.

«Серые шляпы» часто наносят ущерб с целью выявить уязвимости, однако они не представляют особой опасности.

Компания по кибербезопасности Darktrace опубликовала отчет «2018 Threat Report» 31 июоя, в котором подчеркивается, что терминал для парковки подключен к веб-сайтам с содержанием для взрослых, но он фактически не показывал этот контент.

«Неизвестно, каков был мотив злоумышленника», – прокомментировали в Darktrace. – «Мы предполагаем, что хакеры хотели указать на уязвимость в, скажем так, “графический” способ, на который бы не наткнулись несовершеннолетние».

Darktrace использует ИИ для выявления подозрительных действий в сети. Вышеупомянутый инцидент является лишь одним из многих, которые Darktrace отслеживал с прошлого года как часть тревожной тенденции.

В другом инциденте компания обнаружила попытку взлома через устройства IoT на линии производства пищевых продуктов. Все устройства, включая блендеры, слайсеры и упаковочные машины, были скомпрометированы.

«Эти устройства не были подключены к основной ИТ-инфраструктуре», – написали Darktrace в своем отчете. – «Сопоставив эти факторы в реальном времени, ИИ Darktrace обнаружил аномальное поведение и определил, что деятельность является значительным риском для производственной линии организации».

Многие устройства IoT остаются незащищенными и могут представлять угрозу для более широкой сети. Ботнеты для DDoS-атак, как и Mirai, используют все большее количество компрометирующих устройств для флуда сетей с рекордным количеством трафика, чтобы вызывать сбои.

(вгору)

Додаток 12

2.08.2018

Исследование: Telegram Passport уязвим брутфорс атакам

Разработчик криптографического ПО Virgil Security, сообщает, что недавно выпущенный инструмент для идентификации личности Telegram Passport оказался уязвим для брутфорс атаки (Cryptellect).

26 июля Telegram объявила о запуске сервиса Telegram Passport, предназначенного для шифрования персональной идентификационной информации пользователей, и позволяет им делиться своими идентификационными данными с третьими лицами, например, представляющими первичные предложения монет (ICO), кошельки для криптовалюты и любые другие сервисы, кто соблюдает правила идентификации личности клиента (KYC).

Данные пользователей хранятся в облаке Telegram с использованием сквозного шифрования, а затем попадают в децентрализованное облако, которое не может дешифровать персональные данные. Однако в своих недавних исследованиях Virgil Security вызвала озабоченность по поводу защиты данных внутри сервиса Telegram.

Согласно программе Virgil Security, Telegram использует алгоритм хеширования SHA-512, который не предназначен для паролей. По сообщениям, этот алгоритм оставляет уязвимости для брутфорс атак, даже если они «соленые». В криптографии «соль» представляет собой случайные данные, добавленные в качестве дополнительного секретного значения в конец ввода, что увеличивает длину исходного пароля, обеспечивая некоторую дополнительную защиту.

Когда пользователь шифрует персональные данные, они, как сообщает Telegram, загружается в облако, и когда пользователь подтверждает подлинность своей личности в сторонней службе, они расшифровывают эти

данные и повторно шифруют их для учетных данных этой службы. По мнению Virgil Security, все эти факторы способствуют потенциальному воздействию хакерским атакам. Компания объясняет:

«Безопасность данных, которые вы загружаете в облако Telegram, в огромной степени зависит от вашего пароля, поскольку атаки с помощью перебора очень просты для выбранного алгоритма хеширования. И отсутствие цифровой подписи позволяет изменять ваши данные без вас или получателя».

В марте учредители Telegram, Павел и Николай Дуров сообщили, что во втором раунде своего ICO собрали 850 миллионов долларов, направленных на разработку приложения Telegram Messenger и собственной блокчейн-платформы Telegraph Open Network (TON). Позднее в мае план Telegram по запуску ICO был отменен из-за того, что приложение для обмена сообщениями привлекло достаточное количество средств в течение двух своих частных пресейлов.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.