СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(31.10–13.11)

2018 № 19

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(31.10–13.11)
№ 19

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

31. 10.2018
Евген Михалыч
Microsoft добавила в Skype несколько новых функций

Корпорация Microsoft выпустила новую версию Skype, предназначенную для общения с помощью браузера. Разработчики предложили пользователям десктопных и мобильных платформ большее количество полезных функций Skype. Среди них:

– Видеозвонки и демонстрация экрана в HD качестве

– Запись звонков: записанный файл вместе со всеми демонстрациями экрана будет храниться в облаке, а все участники получат уведомление, что звонок записывается

– Панель сообщений

– Галерея: при необходимости можно быстро найти файл, который пользователи чата ранее уже присылали

– Поиск в разговорах: теперь можно легко находить сообщения в текущей беседе.

Установить обновление можно при наличии браузеров Microsoft Edge и Google Chrome. Чтобы активно пользоваться новой версией Skype придется обновиться до Windows 10 или MacOS 10.12 (IT новости).

***

1.11.2018
Crello позволил создавать Instagram Stories с помощью шаблонов

Онлайн-редактор Crello запустил новый формат – видеоистории для Instagram. Теперь в редакторе можно кастомизировать и редактировать шаблоны, созданные профессиональными дизайнерами, чтобы создавать собственные Instagram Stories.

Докладніше

***

1.11.2018
Начался перенос сервиса Workplace by Facebook на отдельный веб-домен

В тот же день, 28 сентября, когда Facebook объявила о прорыве безопасности, затронувшем миллионы пользователей этой соцсети, глава Workplace by Facebook, Жульен Кодорнью (Julien Codorniou), заверил

руководство Walmart в том, что предпринимаются необходимые меры для скорейшего отделения корпоративного бизнеса Facebook от её публичной сети.

Докладніше

***

2.11.2018
Instagram позволил делиться превью IGTV-видео в «историях»

Instagram объявил о новой функции, которая позволит делиться IGTV видео в историях. При нажатии на иконку в виде бумажного самолетика появится опция «Добавить видео в историю», а друзья могут нажать на превью, чтобы просмотреть все видео в IGTV. Ранее пользователи могли добавить лишь ссылку на IGTV видео в бизнес-аккаунтах. Новая функция позволяет делиться предпросмотром IGTV видео в историях аналогично функции, которая разрешает пользователям репостить истории, в которых их упомянули. Напомним, формат длинных видео был запущен в июне этого года (Marketing Media Review).

***

4.11.2018
Facebook открыла доступ к платформе машинного обучения Horizon

Horizon – платформа для машинного обучения с подкреплением, которую активно использует сама социальная сеть. FB утверждает, что это первое решение, способное обрабатывать огромные массивы реальных данных – то есть информации от пользователей ее приложений (InternetUA).

Машинное обучение с подкреплением означает, что для обучения нейросети достаточно обозначить благоприятные и неблагоприятные исходы, после чего система самостоятельно разберется, как максимизировать результат.

Как говорится в блоге FB, платформу Horizon характеризуют уникальные навыки: она работает о огромными наборами данных – миллионами и миллиардами сэмплов, при низкой скорости обратной связи и учитывает, что все эксперименты должны внедряться с осторожностью. Ведь в случае с соцсетью речь идет не о симуляторе, а о поведении конкретных пользователей.

Как отмечает Engadget, Horizon все шире используется самой соцсетью для обучения своих ИИ-алгоритмов, для которых ранее применялся другой подход – обучение с наставником. Среди известных кейсов: советы от виртуального помощника M в приложении Messenger, настройка уведомлений и оптимизация качества потокового видео.

Сейчас обучение с подкреплением чаще всего используется в робототехнике и компьютерных играх. Facebook надеется, что благодаря Horizon эти методы получат применение и в других областях.

Horizon основан на открытых фреймворках PyTorch 1.0, Caffe2 и Spark. Код уже выложен в репозиторий Facebook Research на Github.

***

5.11.2018

Facebook хочет знакомить людей при помощи тотальной слежки

Facebook знает о вас довольно много. Но хочет знать еще больше. Недавно компания зарегистрировала патент, с помощью которого социальная сеть планирует сводить вместе людей, никак не связанных между собой.

Докладніше

***

7.11.2018

Facebook представит расширенную аналитику для Facebook Pages

Facebook тестирует аналитику для аккаунтов Instagram и расширенную аналитику для Facebook Pages, которые запустятся в течение нескольких месяцев. Новая аналитика аккаунтов Instagram даст более исчерпывающие данные, к примеру метрики с более глубоким уровнем вовлечения, которые включают процент удержания и продолжительность активности пользователей, которые взаимодействуют с контентом бренда в Instagram. Возможность создавать сегменты вокруг вовлеченной аудитории и видеть наслоение пользователей, которые загрузили приложение бренда, заходили на вебсайт или взаимодействовали с брендом на странице в Facebook (Marketing Media Review).

Расширенная аналитика для Страниц Facebook дает более широкую картину влияния Страницы, возможность отслеживать, кто взаимодействовал со страницей, кто подписался/отписался, поставил лайк/дислайк и многое другое. Администраторы Страницы смогут создавать новые сегменты аудитории, отслеживать конверсии и путь к покупке, сравнивать демографические данные аудитории по каналу и активности.

***

8.11.2018

Новая функция Facebook позволит удалять сообщения после отправки

Facebook Messenger скоро позволит вам удалить отправленные сообщения в течение 10 минут после того, как вы их отправили (InternetUA).

Как указано в примечаниях к выпуску версии 191.0 клиента iOS Messenger, функция появится «скоро», пишет The Verge.

По сравнению с часом, который Facebook дает на то, чтобы удалить ошибочное сообщение в мессенджере WhatsApp, 10 минут – не слишком много. Но это намного лучше, чем хранить ваши ошибки вечно.

Слухи о «несанкционированной» функциональности Messenger появились с апреля, после того, как Facebook признал, что компания спокойно удаляла сообщения, отправленные ее генеральным директором Марком Цукербергом.

Сейчас в Messenger присутствует функция «Удалить», однако она удаляет сообщения, медиафайлы и переписки лишь у одного пользователя, у второго участника переписки эти данные сохраняются.

***

11.11.2018

Українець запускає анонімну соцмережу для людей з психологічними травмами

Андрій Ключко разом з друзями з Амстердаму запускає анонімну соціальну мережу Turtle для людей, які пережили фізичні та психологічні травми.

Докладніше

***

12.11.2018

Facebook запустила клона TikTok для подростков

Приложение Tik Tok позволяет создавать музыкальные видео с фильтрами и эффектами. Приложение стало очень популярным среди молодежи. Чтобы привлечь молодую аудиторию в сеть, Facebook выпустила собственное приложение Lasso, которое уже доступна на iOS и Android. Lasso позволяет создавать и делиться короткими видео со смешными эффектами. Пользователи могут следить за другими создателями видео, искать контент с помощью хэштегов и пользоваться музыкальной библиотекой, интегрированной в приложение. Созданными видео можно поделиться в Facebook Stories. По данным The Verge, Facebook запустит подобную функцию для Instagram позже в этом году (Marketing Media Review).

***

12.11.2018

В YouTube все больше ложной информации, но многие используют сервис как источник новостей

В свежем исследовании, которое касается аудитории сервиса YouTube и представленного в нем контента, приняли участие 4594 взрослых жителей США (InternetUA).

Большинство пользователей (87 %) опрошенных заявили, что используют YouTube для того, чтобы узнать, как решить ту или иную проблему, найти рецепт, починить что-то и так далее. Более половины людей в возрасте от 18 до

29 лет и 41 % взрослой аудитории старше 65 лет подтвердили, что используют YouTube, чтобы научиться чему-то новому.

Но у YouTube есть и обратная сторона. Трое из пяти опрошенных заявили, что видели видеоролики, в которых люди находились в опасных ситуациях. Две трети респондентов утверждают, что им иногда попадаются видеоролики с откровенно ложным контентом. 15 % человек заявили, что натыкаются на подобные видео регулярно.

Проблема в том, что YouTube является не только платформой стриминга видео, но и местом, откуда многие узнают новости. 53 % опрошенных подтвердили, что открывают YouTube в желании узнать, что важного происходит в мире.

Представители YouTube подтвердили, что в первой половине этого года компания удалила более 17 млн видеороликов, которые нарушают правила сервиса и содержат неприемлемый контент.

***

13.11.2018

В Twitter может появиться одна из самых ожидаемых функций

Компания Twitter думает над тем, чтобы добавить функцию редактирования записей в социальной сети. Об этом сообщает The Next Web (InternetUA).

По словам основателя и главы соцсети Джека Дорси, компания должна тщательно рассмотреть варианты использования кнопки редактирования, прежде чем ввести ее.

«Нужно обратить внимание на то, как может использоваться кнопка редактирования. Многим людям нужна кнопка редактирования, потому что они хотят быстро исправить ошибку. Например, опечатку или ошибку в URL. Это выглядит более реально, чем позволять людям редактировать твиты за все время», – отметил он.

Он добавил, что Twitter не хочет вводить возможность неограниченного редактирования, чтобы люди не злоупотребляли этой функцией и не правили свои записи с противоречивыми заявлениями или словами, которые вызвали осуждение.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

1.11.2018

#СушкоГейт: Как в сетях вспыхнул скандал вокруг плагиата главреда Vogue.UA

В Интернете не стихает скандал вокруг глянцевого журнала Vogue Ukraine. Читатели обнаружили в редакторской колонке плагиат из российских источников. Это уже не первый инцидент с главным редактором украинского издания, ранее ее также уличали в присваивании чужих мыслей.

Докладніше

***

6.11.2018

«Тернопіль без маршруток чудовий». На саботаж перевізників соцмережі відреагували жартами і флешмобами

На вимогу людей міська влада відреагувала поверненням старих тарифів у громадському транспорті. У відповідь маршрутники не вийшли у рейси. Тернополяни не засмучуються і гуртуються, аби добратися на роботу (20 хвилин).

Після підвищення тарифів на проїзд у маршрутках і тролейбусах удвічі, яке було, наче грім серед ясного неба, частина жителів файного міста побігла за «Карткою тернополянина», частина розкупила електронні квитки, і лише найрадикальніші вирішили не коритися. Люди організовували флешмоби на кшталт #пішки_на_роботу, висловлювалися у соцмережах і врешті зібралися на транспортне віче. 5 листопада, під тиском громади міська рада змушена була повернути тарифи до попереднього рівня, аж поки не буде економічного обґрунтування.

***

6.11.2018

В соцсетях стартовал флешмоб в поддержку законопроекта об усилении защиты животных

Активисты зоозащитной инициативы UAnimals объявили о старте флешмоба #депутатголосуй (Одесская жизнь).

Об этом зоозащитники написали на своей ФБ-странице: «Просим всех тегать в комментариях народных депутатов, которых вы знаете с просьбой проголосовать за законопроект 6598, который стоит под номером 6 в повестку дня Верховной Рады в четверг 8 ноября».

Законопроект № 6598 называется «О внесении изменений в некоторые законодательные акты Украины (относительно имплементации положений некоторых международных соглашений и директив ЕС в сфере охраны животного и растительного мира)».

Именно этот законопроект, например, должен запретить попрошайничество с животными и эвтаназию бездомных животных для регулирования их численности.

В целом законопроектом № 6598 предлагается внести ряд изменений в три Закона Украины – «О животном мире» и «О защите животных от жестокого

обращения», «Об охотничьем хозяйстве и охоте», а также в Административный и Уголовный Кодексы Украины. Цель правок – усилить защиту животных от жестокого обращения.

***

8.11.2018

В Одесской области стартовал флешмоб «Я за честные выборы!»

В городе Подольск Одесской области команда депутата городского совета Олега Янчевского запускает конкурс-флешмоб «Я за честные выборы!». Об этом сообщил чиновник на своей странице в Facebook (Одесса Медиа).

Суть конкурса такова: каждый, кто сделает селфи на фоне билборда, расположенного в городе, опубликует в соцсети с хештегом #змінимоміcторазом получит уникальную возможность выиграть батник с логотипом команды. Также в посте отмечено, что для участия в розыгрыше необходимо быть подписанным на паблик команды в Instagram и Фейсбук.

Также Олег Янчевский призвал все города Украины поучаствовать в акции.

***

8.11.2018

«Вова прийде – порядок наведе»: соцмережі вибухнули через нову рекламу з натяком на Зеленського // Користувачі мережі обговорюють нові бігборди гумориста

Користувачі соціальних мереж обговорюють нові білборди з написом «Президент – слуга народу. Незабаром». Щити, що недавно з'явилися в різних містах України, містять натяк на актора Володимира Зеленського. Він зіграв роль президента Голобородька в серіалі «Слуга народу». Соціологи раз у раз включають сатирика до переліку ймовірних претендентів на посаду президента і навіть виводять його у другий тур. Однак сам актор досі не заявив про свою участь у перегонах (Znaj.Ua).

«Якийсь дуже складний ребус на білборді. "Слуга народу" – це у нас серіал про Василя Голобородька. А хто грає роль Голобородька в серіалі – Володимир Зеленський. Значить, відповідь на ребус – "Президент – Володимир Зеленський"», – написав львівський блогер, журналіст і фотограф Роман Голубовський.

«А справді, чому б і не Вова? На тлі старих, обридлих політиків із заводами в Росії і каламутними газовими схемами Зеленський виглядає справді дуже позитивно. То що, Володю, ти ТАК чи НІ?» – запитує блогер Mihail Shnayder.

«Вова прийде – порядок наведе!» – підписав свою світлину на тлі борда співак Іван Марунич.

***

10.11.2018

#пишеморазом: сумчани долучилися до мовного флешмобу

У Сумах долучилися до мовному флешмобу «#пишеморазом», написавши диктант єдності (The Sumy Post).

Щорічний радіодиктант національної єдності писали українці у різних куточках світу. Сам текст, згідно усталеної традиції, прочитав український лінгвіст Олександр Авраменко. Цьогоріч автор обрав тему – «Наші пісні».

Школярі, студенти, викладачі, працівники пенсійного фонду та, навіть, працівники КП«Електроавтотранс» разом писали диктант з усією країною.

Пропонуємо вашій увазі добірку публікацій сумчан, які взяли участь у флешмобі.

***

12.11.2018

Флешмоб SaveOldDoors: в Одессе просят поддержать проект реставрации старинных дверей

В Одессе запустили флешмоб: надо сфотографироваться на фоне любимой городской двери и выложить фото в соцсеть. Таким образом, просят поддержать проект реставрации старинных дверей (УСИ).

Об этом сообщает общественная организация «Мой дом Одесса», передает корреспондент Украинской Службы Информации.

Флешмоб SaveOldDoors – это возможность поддержать проект реставрации старинных дверей Одессы. Все что нужно сделать – выложить в Facebook фото с табличкой SaveOldDoors на фоне любимой двери. Также всех, кого заинтересовал проект, просят проголосовать за него на платформе «Социально активный гражданин».

Если проект наберет максимальное количество голосов, в Одессе не только отреставрируют старинные двери за счет общественного бюджета, но и создадут новый туристический маршрут. Таким образом, обновленные двери станут достопримечательностью.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

31.10.2018

В Facebook рассказали о потерянных пользователях в Европе

Каждый день более двух миллиардов человек пользуются по меньшей хотя бы одним из ресурсов компании Facebook. Об этом заявил генеральный директор корпорации Марк Цукерберг (InternetUA).

Цукерберг отметил, что 2019 год станет для Facebook периодом «существенных инвестиций».

И хотя в глобальном масштабе этот показатель продолжает расти, число активных пользователей социальной сети Facebook в ее европейском сегменте сократилось за июль-сентябрь с 376 до 375 миллионов.

Это может быть вызвано проблемами с имиджем корпорации, ужесточением европейского законодательства по защите персональных данных и скандалами с несанкционированной передачей третьим лицам сведений о клиентах.

Во втором квартале этого года компания также лишилась миллиона пользователей в Европе. В отчетности компании говорится, что общий объем выручки в третьем квартале по сравнению с аналогичным временным промежутком в 2017 году стал больше на 33 процента, или на 13,7 миллиарда долларов.

И в то же время, по данным информагентств, это – минимальный прирост, который показала компания за почти шесть лет. Прибыль увеличилась на девять процентов, достигнув почти 1,34 млрд долларов.

***

31.10.2018

ПриватБанк позволил оплачивать покупки и услуги в Telegram

ПриватБанк интегрировал свою платежную систему LiqPay в платежные методы Telegram Payments, что позволит украинским компаниям принимать платежи с помощью Apple Pay и банковских карт непосредственно в ботах мессенджера, отметила компания у себя на сайте (Marketing Media Review).

«Теперь бизнесу не нужно тратить время, ресурсы, деньги на реализацию сервиса по предоставлению услуг в Интернете, – говорит член правления ПриватБанка Сергей Харитич. – Начать продавать в смартфоне просто и легко – подключи свой магазин в LiqPay, создай бот в Telegram и принимай оплаты».

Первыми украинскими телеграм-ботами, которым ПриватБанк интегрировал новый сервис, стали самый популярный бот для бронирования и покупки железнодорожных билетов @Railwaybot и сервис мониторинга открытых данных госреестров @Opendatabot.

С помощью новых инструментов оплаты пользователи @Railwaybot теперь могут покупать билеты на поезд прямо в Telegram без перехода на веб-страницы билетного сервиса.

Платежный сервис в Telegram доступен всем пользователям последней версии мессенджера.

***

31.10.2018

Burberry меняет стратегию, продавая новинки в Instagram

Модный дом Burberry запустит отдельные продукты в Instagram ради привлечения молодых покупателей. Новый e-commerce шаг – это очередной разрыв с традициями под руководством нового CEO Риккардо Тиши, который занял свою позицию в марте. Ряд продуктов будет также представлен в китайской сети WeChat, корейском сервисе Kakao и японском сервисе Lin, уклонившись от традиционного запуска в магазине или на сайте бренда (Marketing Media Review).

***

1.11.2018

Цукерберг назвал Apple главным конкурентом мессенджеру от Facebook

Глава Facebook Марк Цукерберг назвал iMessage от Apple главным конкурентом компании на рынке мессенджеров. Об этом он заявил во время звонка с аналитиками и журналистами после отчётности за третий квартал 2018 года, передаёт CNBC (InternetUA).

По словам Цукерберга, WhatsApp и Messenger занимают лидирующие позиции на рынках Европы, где продажи Android и iOS примерно на одном уровне, но уступают на таких важных рынках, как американский, где доминируют продажи iPhone.

«Сегодня наш самый большой конкурент – iMessage. В таких важных странах, как США, где позиции iPhone сильны, Apple привязывает iMessage как приложение для обмена текстовыми сообщениями по умолчанию», – Марк Цукереберг, глава Facebook

Сервисами Facebook, включая саму соцсеть, Messenger, WhatsApp и Instagram, пользуются 2,6 млрд людей по всему миру. Цукерберг отметил, что их пользователи отправляют друг другу 100 млрд сообщений в день, а в WhatsApp делятся фотографиями, видео и ссылками чаще, чем в социальных сетях.

***

2.11.2018

В WhatsApp появится реклама

Вице-президент WhatsApp Крис Дениелс подтвердил, что в мессенджере совсем скоро появится реклама (InternetUA).

Как сообщает Outlook India, рекламные вставки будут видны в разделе статусов – там, где пользователи обмениваются короткими видео или фотографиями, которые исчезают через 24 часа.

В Facebook отмечают, что статусами WhatsApp ежедневно пользуется около 450 миллионов человек.

Комментируя нововведение, Крис Дениелс подчеркнул, что это будет основной способ монетизации WhatsApp, а также возможность для компаний получить доступ к аудитории мессенджера.

Стоит отметить, что создатели приложения изначально не планировали монетизировать его с помощью рекламы. Желание соцсети Facebook, нового владельца WhatsApp, зарабатывать на мессенджере, вынудило их покинуть свой проект.

В настоящее время WhatsApp пользуется более 1,5 миллиарда человек во всем мире.

***

5.11.2018

Facebook переориентирует структуру Oculus на дальние перспективы

Компания Facebook продолжает оптимизировать интеграцию Oculus в свою корпоративную структуру с прицелом на массовое внедрение виртуальной реальности в течение следующих десяти лет.

Докладніше

***

8.11.2018

Михаил Сапитон

Как изменилось продвижение «Розетки» в Facebook и Instagram. Кейс от компании Promodo

В 2018 году «Розетка» сильно изменилась. Маркетплейс объединился с EVO Group, изменил айдентику и открыл флагманский магазин в здании Главпочтамта на Крещатике. В блоге компании детально рассказано, как меняли подход маркетплейса к ведению Facebook, Instagram и общению с аудиторией.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

4.11.2018

Исследование подтвердило опасность «гаджетомании» для детской психики

Исследование 40000 несовершеннолетних показало, что часы, проведенные перед экраном компьютера или смартфона влияют на развитие. И для подростков гаджеты даже более опасны, чем для маленьких детей (InternetUA).

Для американского ребенка четыре часа перед экраном в день – это умеренный уровень пользования гаджетами. Но даже такое количество времени перед телевизором, компьютером или с мобильным устройством в руках повышает риск развития у ребенка депрессии, тревожности и других отклонений, показало исследование психологов из Университета штата Калифорния в Сан-Диего и Университета Джорджии.

Дети в США в среднем проводят с гаджетами или перед телевизорами пять-семь часов в день. Для дошкольников зависание перед телевизором очень часто превращается в отсутствие самоконтроля, а также мешает успокоиться, отмечает EurekAlert.

Школьники 11-13 лет, которые растут с гаджетами в руках, становятся нелюбознательными.

Подростки в возрасте от 14 до 17 лет, которые проводили перед экраном более семи часов в день, теряют возможность концентрации на задачах.

«Сначала меня удивило большее влияние на юношей и девушек, – признается Жан Твенж из Университета штата Калифорния. – Но ведь подростки проводят больше времени со своими телефонами и в соцсетях, а мы знаем из других исследований, что такие занятия сильнее коррелируют с ухудшением самочувствия, чем телесмотрение или видеоигры – то, чем занимаются дети».

***

8.11.2018
Ирина Фоменко
Интернет-зависимость ребенка начинается в утробе матери

У детей до 13 лет уже более 1000 фото опубликованы в Интернете, пишет The Telegraph. По словам Комиссара по делам детей Энн Лонгфилд, онлайн-зависимость начинается еще в утробе матери, с того момента, как родители выкладывают УЗИ плода.

Докладніше

***

8.11.2018
Соцсети определяют уровень счастья девушек

Учёные в процессе исследования установили, что уровень испытываемого счастья у современных представительниц прекрасного пола существенно снизился (InternetUA).

К таким выводам пришли представители благотворительной организации под названием Girlguiding. Они провели опрос, участие в котором взяли представительницы прекрасного пола в возрасте от семи до двадцати одного года. Специалистам удалось установить, что на сегодняшний день лишь четверть юных леди может назвать себя полностью счастливыми. Стоит отметить, что десять лет назад абсолютно довольными своей жизнью были сорок девять процентов девочек и молодых женщин. При этом около шестидесяти процентов респондентов признались, что основной причиной, подавляющей их состояние счастья, являются сообщения и критика, распространяемые посредством социальных сетей. Также семьдесят процентов представительниц прекрасного пола назвали фактором грусти предстоящие экзамены и контрольные работы.

Огромное внимание нужно обратить на то, что пятьдесят процентов участниц опроса назвали неудовлетворённость своей жизни главной причиной проблем со здоровьем. Просуммировав всё вышесказанное, можно прийти к выводу, что глобальные процессы в современном мире и большой темп его развития негативно сказываются на психическом состоянии молодых женщин. Поэтому учёным стоит немедленно приняться за поиск путей их эмоциональной разгрузки.

***

12.11.2018

Эксперимент доказал: социальные сети пагубно влияют на здоровье

Экспериментальное исследование, проведенное психологами из Университета Пенсильвании, впервые показало причинную связь между использованием социальных сетей и более низкими показателями здоровья и самочувствия.

Докладніше

Маніпулятивні технології

1.11.2018

Журналистам удалось от имени других людей опубликовать 100 рекламных объявлений в Facebook

Сотрудники издания Vice выдали себя за представителей 100 американских сенаторов и попытались разместить политическую рекламу в социальной сети Facebook. В итоге модераторы, утверждавшие, что сделали все для предотвращения манипуляций, одобрили все объявления (InternetUA).

Одним из основным усилий сервиса Facebook по повышению прозрачности политической рекламы стало обязательное раскрытие

информации «Оплачивается» – с ее помощью пользователи должны понять, что перед ними рекламное политическое объявление, а также кто его заказал.

Оказалось, что такими объявлениями очень легко манипулировать. В этом году журналисты Vice подали заявку на покупку поддельных рекламных постов от имени всех 100 сенаторов США. После того, как рекламные посты были одобрены, их можно было опубликовать в Facebook. Журналисты издания особо отметили, что не воспользовались этим.

***

6.11.2018

Мошенники в Instagram: пользователи ПриватБанка лишаются средств в соцсетях

В нынешнем мире каждый пытается получить денег и при этом ничего не делать. К сожалению, далеко не все пытаются заработать честными путями. Изысканность и креативность мошенников не прекращает преподносить «сюрпризы» доверчивым гражданам (InternetUA).

На этот раз случаи мошенничества распространились через Instagram. Об этом сообщает Информатор со ссылкой на пост в Facebook руководителя пресс-службы ПриватБанка Инны Музычук.

Простыми словами в посте написано, что обычные люди «ведутся» на предложения мошенников. В Instagram создаются фейковые аккаунты ПриватБанка, после чего просят отметить страницу в публикации. Следующим этапом просят прислать номер карты, а финишной прямой становится запрос о том, что карта не подтягивается в систему и пользователя просят дать пароль.

При совершении всех вышеперечисленных действий, ситуация резко меняется, а на счетах денег уже нет. И только потом клиенты банка обращаются в поддержку с жалобой на то, что их средства исчезли магическим образом. В конце Музычук порекомендовала подписываться только официальный аккаунт Приват Банка в Instagram.

***

7.11.2018

Ирина Фоменко

Основные виды предвыборной дезинформации в соцсетях

Фейковые материалы, вводящие в заблуждение объявления и подозрительные почтовые сообщения являются особенностью большинства современных политических кампаний. Но есть еще одна разновидность дезинформации: непосредственно в день голосования появляются слухи, обман и ложные данные.

Докладніше

***

7.11.2018
Ирина Фоменко
Террористы вербуют подростков через онлайн-игры

Некоторые экстремистские группы используют многопользовательские игры и внутриигровые чат-функции для привлечения новых членов. Об этом сообщает The Star Online (InternetUA).

Происходит это не только в играх, но и на платформах вроде Discord и Reddit. Вербуют и во время живых трансляций на Twitch и YouTube.

Почему ксенофобы используют игры для привлечения новых участников? По словам Джоан Донован из Data and Society, сторонники превосходства белой расы раньше уже вербовали членов через онлайн-платформы. «Шутеры от первого лица – это одно из лучших мест для поиска недовольных молодых людей», – заявил Донован.

«Я видел, как экстремистские группы общались с другими, не говоря о том, что они – шовинисты. Ксенофобы выясняют, чем недовольна молодежь, и используют это в социальном движении», – объясняет Джоан.

В то время как игровые платформы наподобие Steam запрещают подстрекательские высказывания, сложно найти группы ненавистников с таким количеством человек. В результате многие платформы полагаются на пользователей, которые самостоятельно должны сообщать о подобных случаях.

Грег Бойд из юридической фирмы Frankfurt Kurnit отметил, что Microsoft, PlayStation и Steam принимают каждый месяц 48 миллионов, 70 миллионов и 130 миллионов активных пользователей.

«Это население Испании, Франции и России. А потом представьте, что вы контролируете все их текстовые и голосовые чаты, буквально на каждом языке и диалекте», – прокомментировал Бойд.

***

8.11.2018
Российские тролли усиливают активность в социальных сетях

Согласно проведенному исследованию компанией New Knowledge, российская активность в социальных сетях лишь увеличилась, несмотря на комплекс мер, предпринятых США. Осуществленные руководством США меры заставили Россию всего лишь изменить тактику.

Докладніше

Спецслужби і технології «соціального контролю»

3.11.2018
Twitter удалил 10 тысяч аккаунтов за призывы игнорировать выборы в США

Twitter удалил 10 тысяч аккаунтов, которые в автоматическом режиме отправляли сообщения с призывами не голосовать на выборах в США. Об этом сообщает Reuters (InternetUA).

Сообщения публиковались от имени сторонников Демократической партии. Аккаунты были удалены в конце сентября и начале октября.

«Мы удалили ряд аккаунтов за попытки публиковать дезинформацию в автоматическом режиме. Это нарушает нашу политику», – заявил CNN представитель компании.

По его словам, сеть аккаунтов была запущена с территории США.

***

4.11.2018

Daily Telegraph рассказала, как Иран и Китай разгромили агентуру ЦРУ с помощью Google

В период с 2009-го по 2013 год ЦРУ США пострадало от «катастрофического» провала, вызванного тем, что иранские власти сумели вскрыть коммуникационную платформу агентства с помощью сервиса Google.

Докладніше

***

5.11.2018

В России хотят создать кибердружины

Депутаты Государственной думы от «Единой России» подготовили законопроект, который предусматривает создание кибердружин. Им надлежит мониторить Интернет и выявлять противоправную и запрещённую информацию.

Докладніше

***

6.11.2018

Спецслужби США у спільній заяві попередили американців про фейкові російські «новини»

Спільною заявою ФБР, Нацрозвідка, Міністерство внутрішньої безпеки та Мін'юст попереджують виборців про російські спроби поширити фейкові новини (Espreso.tv). Відповідну заяву опублікували 6 листопада, передає Deutshe Welle.

«Наразі у нас немає свідчень про спроби злому нашої виборчої системи, які могли б перешкодити голосуванню, змінити кількість голосів або вплинути на їх підрахунок», – наголошується в заяві.

Втім, спецслужби підкреслили, що «деякі закордонні дійові особи», зокрема, Росія, продовжують намагатися вплинути на суспільні настрої та «сіяти розлад».

Опубліковані раніше результати дослідження фахівців з Оксфорда показали, що спроби поширення дезінформації за допомогою соціальних мереж перед виборами в Конгрес мали ширші масштаби, ніж у 2016 році під час виборів президента.

Як зазначає видання, США мають намір вводити санкції проти іноземних громадян і структур за втручання в американські вибори.

***

5.11.2018

СБУ викрила російських ботів, які закликали до повалення влади в Україні

Співробітники Служби безпеки України блокували роботу кремлівських ботів, які закликали до підтримки терористів «Д/ЛНР» та повалення влади в Україні (Espreso.tv).

Про це 5 жовтня повідомила прес-служба СБУ у своєму Facebook.

«Оперативники спецслужби викрили в Одесі, Києві та Сєвєродонецьку дев'ять проросійських пропагандистів. Зловмисники, яких фінансували представники спецслужб РФ, публікували надіслані з Росії політичні новини та закликали до проведення акцій непокори і масових заворушень», – йдеться у повідомленні.

Як зазначили правоохорнці, за задумом російських кураторів через маніпулювання громадською думкою Інтернет-користувачів пропагандисти повинні були впливати на хід проведення майбутніх виборів Президента України.

«Служба безпеки України вкотре звертається до громадян бути уважними, не піддаватись негативному інформаційному впливу з боку підконтрольних спецслужбам РФ пропагандистів та не сприяти зловмисникам у розповсюдженні фейкових "новин" і пропаганди», – наголосили в СБУ.

***

6.11.2018

Facebook заблокував понад сотню акаунтів перед виборами у США

Адміністрація соціальної мережі Facebook заблокувала 115 підозрілих акаунтів напередодні виборів у Сполучених Штатах Америки (Espreso.tv).

Про це повідомила компанія у своєму блозі.

Акаунти були заблоковані, коли американські правоохоронці знайшли зв'язок вказаних сторінок з іноземними державами. Внутрішнє розслідування виявило, що 30 акаунтів Facebook і 85 облікових записів Instagram ймовірно були залучені до «недостовірної діяльності».

«Ми негайно заблокували ці акаунти і зараз проводимо більш детальне розслідування», – заявили в Facebook.

Як зазначається у повідомленні, майже всі сторінки Facebook, пов'язані з цими обліковими записами, французькою або російською мовами, в той час як облікові записи Instagram, в основному були англійською мовою – деякі з них були зосереджені на відомих особах, інших політичних дебатах.

У також компанії зазначили, що у звичайній ситуації перед заявою більш ретельно би проаналізували дані, проте вирішили оприлюднити інформацію про важливі факти, тому що до виборів залишилось небагато часу.

***

6.11.2018

Росіянам блокуватимуть доступ до месенджерів, якщо вони не пройдуть «перевірку»

В Росії затвердили правила ідентифікації користувачів месенджерів за телефоном: тепер усі зареєстровані номери будуть перевірятися через операторів зв'язку (Espreso.tv).

Про це повідомляє російське видання Meduza.

Згідно з документом, користувачам месенджерів заборонено використовувати для ідентифікації чужі номери телефонів. Адміністратори месенджерів повинні перевіряти номери, за допомогою яких реєструються користувачі, через операторів зв'язку, тобто впевнитися, що власник SIM-карти і користувач месенджера це одна і та ж людина.

Як саме це повинно перевірятися, в документі не сказано: придумати такий алгоритм ніби-то мають власники месенджерів. Але якщо росіяни не пройдуть перевірку, то месенджери мають заборонити їм надсилати повідомлення.

У самих операторів буде 20 хвилин на те, щоб підтвердити особистість людини. Згідно документу, користувач не зможе пройти перевірку, якщо оператор не відповість у визначений термін або не знайде відомостей про нього. Користувач також буде повинен пройти ідентифікацію повторно, якщо змінить номер телефону.

***

6.11.2018

Facebook заблокировал предвыборный ролик Трампа

Компания Facebook отказалась размещать предвыборный ролик президента США Дональда Трампа, в котором говорится о связи приближающегося к стране «каравана мигрантов» с преступниками, сообщает CNN (InternetUA).

Отмечается, что видео нарушает рекламную политику соцсети, которая выступает против сенсационного контента.

«Хотя ролик можно опубликовать на Facebook, он не получит платного распространения», – заявили в компании.

Как заявил представитель пресс-службы Facebook, соцсесть имеет определенные стандарты, которые являются особенно строгими для рекламного контента.

***

7.11.2018

У Києві затримали кремлівського інтернет-агітатора, якому в Росії підготували пропагандистську студію

Оперативники Служби безпеки України спільно з прокуратурою АР Крим затримали у Києві інтернет-агітатора, який створив і вів в мережі антиукраїнський канал, повідомила 7 листопада прес-служба СБУ(InternetUA).

Затриманий діяв за вказівкою російських спецслужб. Свій відеоканал він створив у 2015 році і розміщував антиукраїнський контент, який сприяв дестабілізації ситуації в Україні.

В СБУ задокументували поїздки чоловіка в Росію, під час яких він зустрічався зі своїми кураторами, отримував гроші та інструкції, готував створення нових антиукраїнських інформаційних проектів.

Під час обшуку в горе-агітатора правоохоронці знайшли і вилучили цифрове електронне обладнання, а також чернетки із «творчими планами» – сценаріями нових відеороликів.

Оперативники мали інформацію про те, що незабаром чоловік мав намір виїхати в Росію і продовжити свою антиукраїнську діяльність у спеціально облаштованій для нього студії.

Інтернет-агітатору оголошено про підозру у вчиненні кримінальних правопорушень, передбачених ст. 109 (насильницька зміна чи повалення конституційного ладу) і ст. 110 (посягання на територіальну цілісність і недоторканність України) КК України. Триває досудове слідство.

***

7.11.2018

Женщину осудили за антиукраинскую пропаганду в соцсетях

Жительница Северодонецка осуждена за распространение в социальной сети информации с призывом изменить границы территории Украины (InternetUA). Об этом сообщает пресс-служба прокуратуры Луганщины.

Так, на протяжении 2014-2015 годов женщина активно участвовала в антиукраинских группах в социальной сети «ВКонтакте», распространяя информацию с призывами к изменению границ территории Украины в нарушение порядка, установленного Конституцией Украины, путем признания террористической организации «ЛНР» независимой республикой и присоединение части территории Украины в состав Российской Федерации.

В ходе досудебного расследования подозреваемая полностью признала свою вину в совершении инкриминируемого ей уголовного преступления, искренне раскаялась, активно способствовала раскрытию преступления и разоблачению других соучастников.

«Приговором Северодонецкого городского суда Луганской области лицо признано виновным в совершении уголовного преступления, предусмотренного ч. 1 ст. 110 УК Украины, и назначено наказание в виде 3 лет лишения свободы с освобождением от отбывания наказания с испытанием сроком на 2 года и применением специальной конфискации имущества», – сказано в сообщении.

***

7.11.2018

В Facebook связали заблокированные перед выборами аккаунты с Кремлем

В Facebook рассказали, что аккаунты, заблокированные перед промежуточными выборами, вероятно, связаны с «российскими агентами», которые распространяли дезинформацию во время президентских выборов 2016 года. Об этом сообщает Washington Post (InternetUA).

Согласно заявлению компании, удаленные аккаунты связаны с «Агентством-интернет исследований» (IRA), которое считают прокремлевской организацией. Кроме того, руководство соцсети заявило, что связаный с IRA веб-сайт опубликовал список созданных «Агентством» аккаунтов в Instagram.

«Это своевременное напоминание о том, что недобросовестные деятели не сдадутся, и почему так важно, что мы работаем с правительством США и другими технологическими компаниями, чтобы быть впереди», – заявил глава департамента кибербезопасности Facebook Натаниэль Глейхер.

***

12.11.2018

У Франції податкова буде моніторити сторінки неплатників податків у соцмережах // Фото з розкішними авто або на узбережжі Маямі викличуть підозру, чи справді людина така бідна, як прикидається

Якщо громадянин Франції не сплачує податки, але постить у соцмережах фото з розкішними будинками чи автомобілями – він тепер стане об'єктом прискіпливої уваги податкових інспекторів.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

31.10.2018

Против «ВКонтакте» подали первый иск за разглашение правоохранителям персональных данных

Сотрудница штаба российского оппозиционера Алексея Навального Лилия Чанышева подала иск в суд Санкт-Петербурга на администрацию социальной сети «ВКонтакте» за разглашение правоохранительным органам личной информации пользователей.

Докладніше

***

31.10.2018

Полиция рассказала, как обезопасить себя от нового кибермошенничества

Чтобы выманить у клиентов деньги и личную информацию, кибермошенники открывают фейковые банковские сайты и отправляют на электронную почту пользователей фишинговые письма (InternetUA).

Об этом 30 октября сообщает пресс-служба Национальной киберполиции в Facebook.

Правоохранители отмечают, чтобы отличить фейковый сайт от оригинального, нужно обращать внимание на «всплывающие окна» сайта. Так, фейки часто требуют подавать банковские реквизиты, но банковские учреждения так не делают.

Также фейковые сайты могут иметь недостатки оформления, такие как грамматические ошибки.

В полиции советуют не торопиться и не щелкать на подозрительный сайт банка в электронных письмах, а также вводить адрес сайта вручную, или выбирать ссылку из закладок.

***

31.10.2018

Google обновил reCAPTCHA: доказывать, что вы не робот больше не потребуется

Компания Google обновила свою систему защиты сайтов от ботов reCAPTCHA. Новая версия уже доступна для разработчиков. Новая reCAPTCHA v3 больше не требует от пользователей выполнять какие-то действия, будь то выбор картинок с определенным типом изображений или нажатие на кнопку «Я не робот» (IGate).

Теперь система проводит анализ действий пользователя, включая движения курсора мыши, взаимодействие со страницами. Далее происходит оценка собранных данных по шкале от нуля до единицы. Чем выше результат, тем больше вероятность, что посетитель – человек. Администрация сайтов

сможет самостоятельно установить пороговый уровень, при котором будет требоваться дополнительная, более тщательная проверка.

В Google рекомендуют устанавливать обновленную reCAPTCHA не только на странице входа или заполнения какой-либо формы, а сразу на нескольких страницах – это должно помочь лучше и точнее выявлять подозрительные действия и блокировать деятельность роботов.

***

31.10.2018

Google удалила из Google Play 29 банковских троянов

Эксперт антивирусной компании ESET Лукас Стефанко узнал о существовании 29 вредоносных приложений для Android, которым удалось обойти защиту Google Play и закрепиться в каталоге. Все они были ориентированы на кражу учетных данных для доступа к банковским счетам своих жертв.

Докладніше

***

31.10.2018

Михаил Сапитон

Десктопный клиент Telegram хранит переписку в незащищенном виде. Это не компрометирует мессенджер

Первокурсник американского колледжа Wake Technical Натаниэль Сачи публично раскритиковал защищенный мессенджер Telegram. Он обнаружил, что программа хранит содержимое чатов локально, в незащищенном виде и пожаловался на ситуацию в Twitter.

Докладніше

***

31.10.2018

В Швеции тысячи людей вживили себе под кожу упрощающие жизнь чипы

В Швеции наблюдается повальное увлечение биохакингом. Тысячи граждан вживили себе под кожу чипы, в которых хранится личная информация и с помощью которых можно взаимодействовать с окружающей технологической средой. Тенденция пока не планирует сбавлять обороты, но некоторые учёные говорят, что массовое вживление чипов таит в себе ряд опасностей.

Докладніше

***

1.11.2018

Dell EMC Cyber Recovery обеспечит последнюю линию защиты данных от кибератак

Компания Dell EMC представляет ПО Cyber Recovery и сервисы для восстановления и реабилитации, которые помогут обеспечить последнюю линию защиты данных от кибератак и программ-вымогателей.

Докладніше

***

1.11.2018

ПО для мониторинга курса криптовалют тайно устанавливает бэкдоры на компьютеры

Злоумышленники устанавливают бэкдоры на компьютеры под управлением macOS под видом приложения для мониторинга курса криптовалют CoinTicker (InternetUA).

Установив CoinTicker, пользователь может указать, какие криптовалюты его интересуют, и следить за их курсом. На панели меню macOS появится небольшой виджет, отображающий изменения в курсе. Это весьма удобно, если не учитывать тот факт, что в фоновом режиме приложение незаметно загружает два бэкдора, позволяющих злоумышленникам получать удаленный контроль над зараженными компьютерами.

«После запуска приложение загружает и устанавливает компоненты двух разных бэкдоров с открытым исходным кодом – EvilOSX и EggShell», – сообщил Томас Рид (Thomas Reed) из Malwarebytes.

Бэкдоры загружались из репозитория GitHub (в настоящее время репозиторий уже удален). Сначала загружался EggShell. Загрузившись, вредонос создавал лаунчер для автоматического запуска после авторизации пользователя на зараженном компьютере. Затем с помощью обфусцированного скрипта EggShell загружал EvilOSX. Второй бэкдор также создавал лаунчер для автоматического запуска.

Был ли CoinTicker вредоносным изначально, или его скомпрометировали злоумышленники, неизвестно. На сайте отсутствует какая-либо контактная информация для связи с разработчиками, а есть только кнопка для загрузки. Из этого можно предположить, что CoinTicker изначально создавался для вредоносных целей.

***

1.11.2018

Мощный ботнет взялся за сбор писем тысяч жертв

Эксперты в области кибербезопасности из компании Kryptos Logic обнаружили, что новый ботнет Emotet начал сбор всей электронной почты с

захваченных устройств. Об этом специалисты сообщили в блоге организации (InternetUA).

Краже подверглись письма, хранящиеся последние полгода. В частности, были украдены имена получателей и отправителей, их адреса и содержимое каждого сообщения. Ранее этот же ботнет применили для сбора списка контактов. Специалисты полагают, что все полученные данные уйдут в один большой массив.

Точное число жертв ботнета неизвестно. По предварительным данным, заражению подверглись уже несколько десятков тысяч устройств, уязвимыми являются все инфицированные компьютеры.

По словам специалистов, Emotet является одной из наиболее современных и продвинутых ботсетей, которая может принести немалый доход злоумышленникам.

***

2.11.2018

Рекламное ПО и майнеры лидируют в октябрьском рейтинге вирусов

Компания Eset представила тенденции распространения компьютерных угроз в октябре. Согласно данным, полученным с помощью системы быстрого оповещения Eset LiveGrid, топовые позиции в рейтинге наиболее активных вредоносных программ занимает рекламное ПО и угрозы для скрытой добычи криптовалюты.

Докладніше

***

2.11.2018

Google придумала новый способ борьбы с вирусами на Android

Нововведение предусматривает задействование JavaScript для сканирования устройства на предмет вредоносных компонентов, препятствуя авторизации во избежание кражи учетных данных мошенниками с целью последующей компрометации аккаунта и его использования в личных целях.

Докладніше

***

2.11.2018

Українець розсилав комп’ютерний вірус під виглядом розважальних програм

Працівники Причорноморського управління Департаменту кіберполіції викрили мешканця Миколаєва у розповсюдженні шкідливого програмного забезпечення. Завдяки модифікації вірусу зловмисник дистанційно керував

комп’ютером жертви, а також отримував доступ до веб-камери інфікованого комп’ютера.

Докладніше

***

4.11.2018

На промышленных USB-накопителях обнаружены опасные вирусы

USB-накопители представляют серьезную угрозу промышленным системам и могут использоваться для вмешательства в работу сервисов энергетических компаний, предприятий коммунального водоснабжения и других организаций в сфере критической инфраструктуры.

Докладніше

***

4.11.2018

Демократическую партию США обвинили в хакерской атаке на избирательную систему

Демократическую партию США в штате Джорджия обвинили в попытке взломать систему регистрации избирателей накануне губернаторских выборов. Об этом сообщает NBC (InternetUA).

С обвинением выступил кандидат от республиканцев, госсекретарь штата Брайан Кемп. Он заявил, что Демократическая партия предприняла «неудачную попытку взломать систему регистрации избирателей штата». Кемп добавил, что его офис ведет расследование по этому поводу и уже предупредил ФБР и Министерство внутренней безопасности.

«Я могу подтвердить, что Демократическая партия в Джорджии находится под следствием за возможные киберпреступления», – заявил Кемп.

Представители демократов назвали заявления Кемпа «политическим трюком».

***

4.11.2018

Хакеры готовят атаки на энергетический сектор Украины

Специалисты по кибербезопасности предупреждают о новых готовящихся атаках, которым будет подвергнут в первую очередь энергетический сектор страны. Война идет не только на восточном фронте в Донбассе и на складах боеприпасов. И если в других странах «политические» хакеры влияют прежде всего на выборы, то в Украине удары приходятся на жизненно важные объекты инфраструктуры (InternetUA).

Об этом в своей статье для ZN.UA пишет Герман Богапов. По его словам, организованная, но пока так и не обнаруженная, группа злоумышленников осуществляет целевые атаки на объекты в стране в течение нескольких лет.

«Анализируя объекты и время атак, а также то, что они осуществляются именно в нашей стране, несложно понять, что кибератаки являются еще одним оружием Кремля в войне против Украины», – подчеркивает автор.

***

5.11.2018

Хакери атакували австралійське військове підприємство Austral

Невідомі кіберзлочинці атакували австралійське оборонне суднобудівельне підприємство Austral (Espreso.tv). Про це повідомляє news.com.au.

Хакери вкрали номери мобільних електронів у адреси електронної пошти деяких працівників компанії, після чого вимагали за них гроші та намагалися продати в інтернеті.

У компанії наголосили, що зловмисникам не вдалося викрати жодних даних щодо нацбезпеки або роботи підприємства.

«Наразі немає жодних відомостей, що до рук злочинців потрапили дані, що стосуються національної безпеки або комерційної діяльності компанії», – заявляє Austral.

Компанія повідомила уряд країни про інцидент. Австралійський центр кібербезпеки та поліція почали розслідування атаки.

Австралійське Міноборони також заявило, що жодного витоку важливих даних не відбулося, проте закликало до пильності та наголосило на необхідності партнерам у галузі посилювати кіберзахист.

***

5.11.2018

Американські вчені розробили дієву програму для боротьби із кібершахраями

За допомогою нової програми дослідники допомагають правоохоронним органам боротися з шахраями, які крадуть дані електронних поштових скриньок.

Докладніше

***

5.11.2018

Ирина Фоменко

Боты обманывают покупателей на деньги, используя их персональные данные

Великобритания начинает расследование использования персональных данных для установления индивидуальных цен на праздники, автомобили и товары для дома в связи с растущими опасениями об обмане потребителей.

Докладніше

***

5.11.2018

США допомагають Україні підвищити рівень кібербезпеки

Україна в межах угоди USAI ITI отримала допомогу із підвищення рівня кібербезпеки (InternetUA).

Про це повідомив начальник військ зв'язку, начальник Головного управління зв'язку та інформаційних систем Генерального штабу Збройних сил України (ЗСУ) Володимир Рапко в інтерв'ю виданню Міноборони «Телеком. Військовий зв'язок» (жовтень 2018 року).

«На цей час ми вже отримали допомогу з підвищення кібербезпеки Збройних сил України від уряду США в рамках угоди USAI ITI. Прямо зараз проводяться роботи з монтажу обладнання та інсталяція програмного забезпечення у Центрі оперативного реагування на кіберінциденти», – сказав він.

Рапко також поінформував, що спільно з естонськими колегами розроблено проект зі створення кіберлабораторії на базі однієї з військових частин ЗСУ.

«Цей проект схвалено більшістю країн НАТО, зараз ми ведемо перемовини щодо фінансування цього проекту», – пояснив він.

***

5.11.2018

В Стэнфорде изобрели надежный метод шифрования персональных данных

Все пользователи сталкиваются с тем, что программа или устройство запрашивает разрешение на отправку данных разработчикам. Запрет этого действия на самом деле неэффективен – в ПО часто встроены механизмы передачи информации разработчику.

Докладніше

***

6.11.2018

Обережно, за вами слідкують: як онлайн-технології шпигують за людьми

Мобільний телефон знає про вас все. Які дані збирають про користувачів Facebook, Google та мобільні додатки, чи прослуховують оператори ваші дзвінки та поради, як захистити свою інформацію?

Докладніше

***

7.11.2018

Макрон предложил создать «общеевропейскую армию» по кибербезопасности

Президент Франции Эммануэль Макрон предложил создать независимую от США «общеевропейскую армию», в том числе по вопросам кибербезопасности (InternetUA).

По его словам, Европа должна защищать себя сама, без помощи США.

Макрон подчеркнул, что в настоящее время Европа сталкивается с многочисленными попытками вмешательства в киберпространство.

«Сегодня мы видим учащающиеся попытки вмешаться в наше киберпространство и нашу демократическую жизнь. Мы должны защищаться!», – добавил он.

***

6.11.2018

В Японії з'являться «розумні» банкомати, які боротимуться із шахрайством

Японська компанія Hitachi випустить банкомат зі штучним інтелектом і системою розпізнавання осіб, який зможе самотужки запобігати злочинам (Espreso.tv).

Як пише The Mainichi, він дозволить боротися з шахраями.

Після початку роботи з банкоматом нейромережа оцінить зовнішність людини і порівняє її фотографію з базою клієнтів банку, власником картки якого вона є.

Система у разі виникнення підозр може попросити клієнта перервати телефонну розмову (яку може підслуховувати), зняти сонцезахисні окуляри, шарф або шапку. Якщо клієнт відмовиться,то не зможе зняти гроші або провести інші операції.

Система камер дозволяє нейромережі оцінювати поведінку і міміку людини. До того ж, банкомат має доступ до поліцейських баз і зможе розпізнати користувача, раніше засудженого за шахрайство.

«Нова функція банкомату є дійсно інноваційною, оскільки сама машина може допомогти запобігти злочинам. Ми очікуємо, що це буде дуже ефективно», – йдеться у заяві компанії.

***

6.11.2018

Хакери атакували сайт Міністерства з питань тимчасово окупованих територій

Сайт Міністерства з питань тимчасово окупованих територій і внутрішньо переміщених осіб України зазнав кібератаки (Espreso.tv).

Про це повідомила прес-служба міністерства.

Як повідомляється, 2 та 3 листопада невідомим зловмисникам вдалося отримати доступ до панелі управління сайтом. У результаті низку сторінок сайту було модифіковано для поширення спаму. На даний час атаку зупинено, повідомляють у МінТОТ.

«Доступ до панелі керування сайту обмежено, модифіковані сторінки було відновлено до останньої збереженої версії. Триває аналіз втраченої інформації», – інформують у міністерстві.

Представники МінТОТ розповіли також, що це не перші кібератаки на сайт відомства. Так, протягом останніх кількох місяців хакери робили неодноразові спроби зламати акаунти міністерства в соціальних мережах.

У відомстві вважають, що до атаки були причетні російські хакери.

***

7.11.2018

Они читают ваши сообщения: как найти безопасный мессенджер

Вы уверены, что ваша переписка в мессенджере не интересует киберпреступников? Обычно люди думают, что хакеры охотятся за переписками президентов и за аккаунтами директоров корпораций. Но госструктуры и корпорации выстраивают сложные системы безопасности и часто используют для общения закрытые каналы. А вот «рядовые» пользователи общаются в удобных и привычных мессенджерах – не особенно беспокоясь об их безопасности. Взломать их ничего не стоит.

Докладніше

***

7.11.2018

Новая версия Opera для Android позволяет блокировать назойливые уведомления

С 7 ноября пользователи могут улучшить свой опыт работы в сети, скачав последнюю версию браузера Opera на свой смартфон или планшет Android. В новой версии браузера Opera появился встроенный блокировщик окон об использовании cookie-файлов, который при активации блокирует все такие окна на том или ином сайте.

Докладніше

***

8.11.2018

Як смартфон стежить за вами

Маленькі пристрої, які кожен носить у кишені, не лише постачають своїм власникам інформацію, але й збирають її. В кінці 2017 року стало відомо, що Google стежить за користувачами Android.

Докладніше

***

9.11.2018

Пользователей одного из популярных мессенджеров запугали видеороликом-«убийцей»

В WhatsApp активно распространяется сообщение об опасном ролике, который может удалить все данные со смартфона. Эксперты безопасности Sophos в своем блоге написали, что такого видео не существует (InternetUA).

В сообщении говорится, что в скором времени в мессенджере начнет распространяться опасный ролик под названием martinelli.

«Не открывайте видео, оно взломает ваш телефон, и починить его будет невозможно. Распространите это по всему миру», – написано в послании, которое получили множество пользователей сервиса. Спамеры также уверяли, что об опасном вирусе уже говорят в новостях.

Специалисты знакомились с сообщением и назвали его «мусором». По словам экспертов, видео martinelli – вымышленная угроза. Они также отметили, что подобные спам-рассылки начались с середины 2017 года и продолжаются до сих пор.

«Учитывая, что никакого ролика martinelli не существует, пользователи WhatsApp в безопасности от него», – написали исследователи из Sophos. Они также попросили юзеров воздержаться от пересылки этого сообщения.

***

9.11.2018

В Украине заблокировали пиратский киносайт

Работники киберполиции разоблачили автора и заблокировали киносайт «onemov.net» (Espreso.tv). Об этом сообщает пресс-служба Нацполиции.

Владелец пиратского сайта воспроизводил и распространял аудиовизуальные произведения. Права на эти произведения принадлежат компании Universal City Studios LLLP (Universal), представителем в Украине является Украинская антипиратская ассоциация.

Сайт посещали не только украинцы, ведь большинство фильмов, которые размещены на этом ресурсе были на английском языке. Фильмы также

появлялись на русском и украинском языках. Так, охват аудитории увеличивался, в свою очередь, увеличивались и прибыли.

Работники киберполиции и следователи полиции Киевщины, узнали, что администратор пиратского сайта «onemov.net» из Запорожья. Они провели обыск в его квартире и изъяли системный блок компьютера, в котором электронная панель администрирования сайта.

Кроме того, правоохранители обнаружили маршрутизатор, который администратор сайта использовал для администрирования сайта, и банковские карты, на которых средства от размещения рекламы.

Полиция открыла Уголовное производство по ч. 3 ст. 176 (нарушение авторского права и смежных прав) Уголовного кодекса Украины. Задержанному грозит лишение свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. Правоохранители проверяют его причастность к созданию еще около 10 таких сайтов.

***

9.11.2018

Google рассказала о борьбе с пиратством: из результатов поиска удалено более 3 млрд ссылок

Интернет-гигант Google обнародовал отчёт, в котором отражена статистика борьбы с пиратством во Всемирной сети (InternetUA).

Компания отмечает, что на развитие технологий, инструментов и ресурсов, предотвращающих нарушение авторских прав, выделяются значительные средства. «На сегодняшний день наши сервисы позволяют авторам и правообладателям зарабатывать средства, помогают пользователям находить интересный контент и эффективно борются с интернет-пиратством», – заявляет Google.

Итак, в отчёте «Как Google борется с пиратством» за 2018 год приводятся следующие данные. После запуска инструмента для отправки жалоб от правообладателей и их агентов из результатов поиска были удалены в общей сложности более 3 млрд ссылок в связи с нарушением авторских прав.

Количество рекламных объявлений, отклонённых Google в 2017 году из–за подозрений в нарушении авторских прав или из-за наличия ссылок на сайты, нарушающие авторские права, превысило 10 млн.

Тем, кто замечен в нарушении авторских прав, Google запрещает использовать свои рекламные инструменты и системы монетизации. Параллельно компания разрабатывает и внедряет сервисы, упрощающие доступ к легальному контенту.

«Наши усилия довольно эффективны: уровень интернет-пиратства в мире снижается, а затраты на легальный контент всех категорий растут», – говорит интернет-гигант.

Отмечается, что в период с октября 2017 года по сентябрь 2018-го видеохостинг YouTube выплатил более 1,8 млрд долларов США правообладателям в музыкальной индустрии в виде доходов от рекламы.

***

12.11.2018

Владимир Кондрашов

Полиция поймала украинца, который 8 лет продавал «орудия взлома»

Гражданин Украины около восьми лет через собственный интернет-магазин и на специализированных форумах в даркнете продавал так называемые «дедики» (dedicated server – удаленный сервер с мощной аппаратной конфигурацией, используемый злоумышленниками для брута, спама, флуда, DDoS-атак и т. д.). Найти злоумышленника удалось только сейчас.

Докладніше

***

12.11.2018

Злоумышленники атакуют сайты на WordPress через популярный плагин

Киберпреступники активно эксплуатируют уязвимость в популярном плагине WP GDPR Compliance для установки бэкдоров и перехвата управления сайтами на WordPress. Данный плагин помогает владельцам ресурсов обеспечить соответствие требованиям Общего регламента по защите данных (GDPR), число его установок превышает 100 тыс.

Докладніше

***

12.11.2018

Почему не стоит пользоваться сторонними клиентами Telegram

Альтернативные клиенты Telegram могут быть небезопасны, подвергая риску переписку своих пользователей, сообщают авторы канала «Телеграм Технарь».

Докладніше

***

13.11.2018

Интернет превратился в барахолку краденых цифровых профилей

Массовый взлом информационных баз и присвоение цифровых профилей стало сегодня обыденностью. Для получения данных учетных записей кибермошенники применяют фишинговые атаки, недоработки в коде ПО и другие распространенные методы (InternetUA).

«Лаборатория Касперского» опубликовала данные о нелегальных рынках Даркнет, где говорится, что краденые цифровые профили имеют мизерную стоимость. Всего за доллар можно приобрести полный пакет данных, включающий платежные и банковские реквизиты, доступ к соцсетям и разным приложениям, инсталлированным конкретной личностью на ПК или мобильном гаджете.

Цифровая личность сегодня позволяет киберпреступникам проворачивать разные махинации, в том числе и с применением криптовалют, через учетные данные другого человека. Мошенники, занимающиеся реализацией цифровых профилей, даже предлагают скидки оптовым покупателям, и в случае блокирования аккаунта гарантируют получение бесплатной замены.

Столь легкая доступность краденной цифровой личности в Интернете провоцирует усложнение проблем, связанных с защитой конфиденциальности в Паутине. Согласно прогнозам, 75 % экспертов уверены, что человечество встанет перед проблемой обеспечения защиты онлайн–личности и конфиденциальности уже в ближайшем будущем.

ДОДАТКИ

Додаток 1

1.11.2018

Crello позволил создавать Instagram Stories с помощью шаблонов

Онлайн-редактор Crello запустил новый формат – видеоистории для Instagram. Теперь в редакторе можно кастомизировать и редактировать шаблоны, созданные профессиональными дизайнерами, чтобы создавать собственные Instagram Stories (Marketing Media Review).

Каждый шаблон создан в оптимальном для stories размере 1080 на 1920 пикселей, содержит изображения, видео и тексты, которые можно менять под различные задачи. Видеоистории можно скачать в формате mp4, а также загрузить прямо в Facebook Ads Manager, если вы планируете запустить рекламу в Instagram Stories.

Более 400 миллионов пользователей ежедневно просматривают stories в Instagram. Регулярное пополнение аккаунта историями может быть полезно для бизнеса, чтобы нарастить аудиторию, увеличить ее вовлечение в жизнь бренда и создать больше поводов для эмоциональной связи с вашим продуктом. Создание нового качественного контента для stories может отнимать много ресурсов, но Crello с его шаблонами и библиотекой из более чем 65 миллионов фото и видео, поможет значительно упростить этот процесс.

Кастомизация шаблона занимает всего несколько минут. Этот инструмент пригодится предпринимателям или маркетологам, у которых мало времени для генерации идей или создания собственного Instagram контента с нуля.

Наряду с использованием шаблонов пользователи Crello, могут разрабатывать собственные оригинальные дизайны, используя фото, видео, анимированные фоны и анимированные объекты. Кроме того, в stories можно добавлять статичны естикеры и множество дизайн-элементов: линии, границы, логотипы, стрелки, текстовые блоки и т. п.

Коллекция шаблонов Crello для видеоисторий в Instagram постоянно дополняется новыми работами от профессиональных дизайнеров.

Статические шаблоны в Crello можно отредактировать и скачать бесплатно, в то время как большинство форматов с анимацией и видео доступны в платной подписке на PRO аккаунт. Пользователи PRO получают полный доступ к четырем видеоформатам: Анимированная публикация, Full HD видео, видеообложка для Facebook, Instagram стори, а также к коллекции видео, анимированных фонов и объектов.

(вгору)

Додаток 2

1.11.2018

Начался перенос сервиса Workplace by Facebook на отдельный веб-домен

В тот же день, 28 сентября, когда Facebook объявила о прорыве безопасности, затронувшем миллионы пользователей этой соцсети, глава Workplace by Facebook, Жульен Кодорнью (Julien Codorniou), заверил руководство Walmart в том, что предпринимаются необходимые меры для скорейшего отделения корпоративного бизнеса Facebook от её публичной сети (Компьютерное Обозрение).

Walmart является крупным клиентом Workplace by Facebook, платной деловой версии популярной социальной сети, в которой служащие компаний могут общаться между собой в знакомом им стиле Facebook – используя приватные сообщения, ленты новостей и потоковые трансляции. Согласно статистике, обнародованной Facebook год назад, сервис Workplace, конкурирующий со Slack, используют 30 тыс. организаций, включая Starbucks и Chevron.

«Нам гарантировали, что данные находятся за пределами потребительской версии Facebook, что разделение идёт сверху донизу, вплоть до изменения доменного имени», – сообщил вице-президент Walmart, Джоэ Парк (Joe Park).

Спустя месяц, новый домен Workplace.com вступил в строй. Сейчас по этому адресу находится маркетинговый веб-сайт, а его использование в качестве отправной точки для клиентов Workplace by Facebook начнётся в 2019

году. Об этом объявил в интервью CNBC Люк Тейлор (Luke Taylor), продуктовый менеджер Workplace by Facebook. «Мы хотим сделать это с точки зрения бренда, но, как я думаю, это также даст нашим клиентам больше доверия к самому продукту», – сказал он.

Ожидается, что первыми новый домен начнут осваивать новые клиенты, а уже существующие клиенты смогут мигрировать на него постепенно, с той скоростью, которая устраивает их. Спикер Facebook сообщает, что работы по размежеванию потребительского и корпоративного бизнесов компании начались почти год назад.

(вгору)

Додаток 3

5.11.2018

Facebook хочет знакомить людей при помощи тотальной слежки

Facebook знает о вас довольно много. Но хочет знать еще больше. Недавно компания зарегистрировала патент, с помощью которого социальная сеть планирует сводить вместе людей, никак не связанных между собой.

Ни для кого не секрет, что Facebook интересуется знакомствами пользователей. И чтобы выяснить, с кем человек может быть знаком в реальной жизни, соцсеть заглядывает в списки контактов в телефоне, следит за вашей активностью в группах, просматривает фотографии. Именно благодаря этому формируется список людей, которых вы можете знать (IGate).

Сама функция «Вы можете их знать» появилась еще в 2008 году. За десять лет алгоритмы подбора людей стали настолько точными, что иногда от этой точности становится немного жутко. Но теперь ситуация может стать еще более необычной.

Реальные связи

Новый патент описывает систему, которая отслеживает, как часто люди пересекаются в реальном мире. Предполагается, что приложение Facebook будет использовать все типы сигналов смартфона (включая системы Bluetooth, Z-Wave or Zigbee, NFC or PAN), чтобы определять, какие пользователи часто и регулярно оказываются поблизости. Приложение будет фиксировать продолжительность и время встреч. Также может использоваться гироскоп и GPS, чтобы определять, путешествуют пользователи в общественном транспорте, сидят в кафе или прогуливаются пешком.

С помощью всех этих данных алгоритм Facebook сможет определять реальную связь между пользователями, которые никак не пересекаются на виртуальных просторах соцсети.

Благие намерения

Конечно же, сами представители Facebook считают, что подобная система принесет исключительно пользу. Патент утверждает, что функция поможет пользователям, которые повстречали интересного человека, но не получили его контактов. К примеру, вы познакомились с кем-либо на вечернике, но забыли

обменяться телефонами. Другой пример – два человека, которые регулярно ездят на одном автобусе, но теряют контакт, когда один из них меняет маршрут.

Тем не менее, не все разделяют подобный энтузиазм. По мнению правозащитников, такая технология опасно размывает грань между реальной жизнью и виртуальным аккаунтом. Так, представитель правозащитной организации Access Now Эми Степанович пишет, что возможность перемещаться в реальном мире, сохраняя хотя бы некоторую степень анонимности и приватности является важной гарантией безопасности личности.

Функция «Вы можете их знать» даже в том виде, в каком она существует сейчас, уже не раз становилась причиной скандалов. К примеру, алгоритм предлагал «подружиться» больным, анонимно посещающим одного и того же психиатра, раскрывал личности людей из анонимных групп поддержки, выдавал личные данные секс-работниц их клиентам.

В 2016 Facebook уже отрицал, что список «Вы можете их знать» формируется с учетом данных геолокации. Тем не менее, компания признавала, что некоторое время тестировала такую возможность в прошлом. Увы, точный механизм работы алгоритма не известен никому за пределами Facebook.

На данный момент описанная технология слежки за встречами в реальном мире существует лишь в виде патента. Но уже сама возможность реализации чего-то подобного выглядит довольно жуткой. А еще сильнее пугает то, что существование подобной системы может быть выгодно большому количеству людей. К примеру, диктаторским режимам, чрезмерно любопытным спецслужбам или вездесущим рекламодателям.

(вгору)

Додаток 4

11.11.2018

Українець запускає анонімну соцмережу для людей з психологічними травмами

Андрій Ключко разом з друзями з Амстердаму запускає анонімну соціальну мережу Turtle для людей, які пережили фізичні та психологічні травми (Експрес).

Проект розрахований на людей, які самі переживають наслідки травм і не можуть відкрито про них розповісти, пише The Village.

«Припустимо ви відчували або відчуваєте деяку проблему, про яку ви не можете говорити зі своїм партнером, сім'єю або друзями. На нашому сайті ви можете це розповісти іншим людям, які пережили таку ж проблему або переживають зараз», – розповідає Андрій Ключко.

Соціальна мережа буде повністю анонімною та безкоштовною. При реєстрації необхідно буде вказати свій вік, стать, місце проживання. Це необхідно для того, щоб система допомагала шукати людей зі схожими проблемами.

Після реєстрації користувач заповнює так звані scars (шрами – англ.) – травми або проблеми, з якими стикнувся. «Він може коротко вказати свою проблему, наприклад, алкоголізм, або ж розповісти свою історію більш детально», – коментує Андрій Ключко.

Далі можна буде додавати у друзі людей зі схожими проблемами та обговорювати їх у чаті.

До створення Turtle можуть долучитися всі охочі. Для цього потрібно пройти опитування на сайті, щоб засновники могли краще зрозуміти потреби аудиторії.

Також у майбутньому ресурс дозволятиме шукати у місці вашого проживання необхідних спеціалістів для вирішення проблеми. Таким чином, розробники хочуть монетизувати проект.

Нині проект зорієнтований на аудиторію скандинавських країн, проте навесні 2019 року, імовірно, з'явиться російськомовна версія сайту.

(вгору)

Додаток 5

1.11.2018

#СушкоГейт: Как в сетях вспыхнул скандал вокруг плагиата главреда Vogue.UA

В Интернете уже второй день не стихает скандал вокруг глянцевого журнала Vogue Ukraine. Читатели обнаружили в редакторской колонке плагиат из российских источников. Это уже не первый инцидент с главным редактором украинского издания, ранее ее также уличали в присваивании чужих мыслей (InternetUA).

#Буквы восстановили хронологию произошедшего.

Все уже придумали до нас

Подписчики Telegram-канала «Киев Фешн Лавэз» заметили, что редактор украинской версии журнала Vogue Ольга Сушко позаимствовала отрывки из статей шеф-редактора российского издания Harper's Bazaar Шахри Амирхановой двенадцатилетней давности. После разгоревшегося скандала Сушко принесла свои извинения за случившееся, объяснив это тем, что из-за нехватки времени поручила написать текст фрилансеру, а тот скопировал текст Шахри Амирхановой.

На этот раз в новом номере Vogue в колонке главного редактора оказался скопированным не целый текст, а лишь абзац все той же Шахри Амирхановой (с ее странички в livejournal), а также высказывания Геннадия Иозефавичуса и Марины Прохоровой. Всего плагиат был обнаружен в 6 из 10 номеров украинской версии Vogue.

По утверждениям самой Шахри, у нее нет ЖЖ, то есть получается, что заимствованный текст Сушко является копией копии.

Но на этом пользователи соцсетей не остановились и начали искать другие примеры плагиата Сушко, подписывая их #СушкоГейт. Поэтому эта

история переросла в своеобразный флешмоб – кто больше соберет доказательств плагиата Сушко.

Журналистка Алена Мельник написала в Facebook о том, что Сушко еще работая в издании «Коммерсант» использовала чужие мысли, выдавая их за свои.

Подписчики Telegram-канала «Киев Фешн Лавэз» прислали образец плагиата Сушко на текст легендарного кинокритика Андрея Плахова.

Другие попытки плагиата включали в себя отрывки статей из таких изданий, как «Коммерсант», «Сноб».

В свою очередь, Ольга Сушко воздерживается от каких-либо комментариев и не пытается оправдаться за копипаст. А пользователи соцсетей разделились на тех, кто требует увольнения шеф-редактора, и тех, кто пытается ее защитить от нападок.

Данная ситуация продемонстрировала, насколько сложно сегодня выдать чужие мысли за собственные. В эпоху Интернета каждое слово проверяется и перепроверяется тысячами пользователями всемирной Сети. И даже если попытаться воспользоваться материалом многолетней давности его все равно найдут, покажут, проанализируют и обман раскроется.

Если бы подобная ситуация произошла на Западе, то главного редактора издания, скорее всего, ожидали бы крупные неприятности, вплоть до увольнения.

Стоит отметить, что 31 октября поздно вечером вышло совместное заявление медиахолдингов Condé Nast International и ООО «Медиа Группа Украина», которые назначили служебную проверку относительно плагиата в Vogue UA. Главный редактор журнала Vogue Ukraine Ольга Сушко отстранена от должности на время проверки.

(вгору)

Додаток 6

5.11.2018

Facebook переориентирует структуру Oculus на дальние перспективы

Компания Facebook продолжает оптимизировать интеграцию Oculus в свою корпоративную структуру с прицелом на массовое внедрение виртуальной реальности в течение следующих десяти лет. По данным из двух конфиденциальных источников, на этой неделе Facebook изменит принцип группирования команд дополненной (AR) и виртуальной (VR) реальности. Если раньше они были ориентированы на конкретные продукты, то теперь функциональное разделение будет основано на технологиях (Компьютерное Обозрение).

Хотя планируемые перестановки не приведут к увольнениям, они помогут устранить избыточность за счёт объединения специалистов в работе над долгосрочными целями, вместо того, чтобы разделять их по группам, не заглядывающим в будущее дальше следующего гаджета.

Со своей стороны Facebook подтвердила информацию о реорганизации. Спикер компании заявил следующее: «На этой неделе мы внесли некоторые изменения в организацию AR/VR. Это были внутренние изменения, которые не повлияют на потребителей или наших партнеров в сообществе разработчиков».

Технический директор Oculus, Джон Кармак (John Carmack) и сооснователь компании, Нат Митчелл (Nate Mitchell), недавно назначенный главой направления VR для ПК, сохранят свои руководящие должности и будут подчиняться вице-президенту по AR/VR, Эндрю Босворту (Andrew 'Boz' Bosworth).

Новая метаморфоза свидетельствует, что Facebook даже после поведённых ею в этом году масштабных перестановок среди административного состава, осталась неудовлетворена состоянием бизнеса Oculus и считает, что он может развиваться лучше. Разделение по областям компетентности уместно для грандиозных проектов, которые не могут себе позволить распылять силы, а с другой стороны, это может затруднить доступ других команд к новейшим практикам и достижениям. В процессе создания Facebook своей первой полной линейки шлемов-очков VR/AR наблюдается значительное дублирование в технологических проблемах и продуктах у тех, кто работает над решениями для ПК и для мобильного применения.

На днях стало известно, что новый шлем Rift с возможным названием Rift S предполагается выпустить уже в 2019 г. Проект Rift 2 с кодовым именем Caspar, по неофициальным сведениям, был отложен в результате реорганизации. СМИ пока не располагают информацией о том, как она отразится на будущем других продуктов или концептов Oculus.

(вгору)

Додаток 7

8.11.2018

Михаил Сапитон

Как изменилось продвижение «Розетки» в Facebook и Instagram. Кейс от компании Promodo

В 2018 году «Розетка» сильно изменилась. Маркетплейс объединился с EVO Group, изменил айдентику и открыл флагманский магазин в здании Главпочтамта на Крещатике. Однако в компании произошли и менее громкие трансформации. После обновления фирменного стиля, у «Розетки» сменился и соцмедиа-контент. За продвижение бренда в соцсетях отвечало агентство Promodo (AIN.UA).

В блоге компании детально рассказано, как меняли подход маркетплейса к ведению Facebook, Instagram и общению с аудиторией. Редакция AIN.UA приводит кейс целиком.

С узнаваемостью у «Розетки» проблем нет – это самый популярный магазин электронной и бытовой техники в Украине с посещаемостью на уровне 800000 человек в сутки. Promodo предстояли другие задачи:

– изменить контент стратегию, сделать акцент на полезно-информативных публикациях;

– уйти от шаблонных акций.

Каждая из двух ведущих соцсетей потребовала своего подхода.

Facebook: польза и новый рубрикатор

Нужно было подать «Розетку» как маркетплейс – место, где можно купить все что угодно. Для этого потребовалось объединить товарные категории в группы и сформировать под каждую из них целевую аудиторию. Также, специалисты постепенно уменьшили количество акций.

В январе их было 105, в июле – всего 45. Рекламных публикаций с акциями тоже стало на треть меньше. Ссылки на спецпредложения упаковывали в полезные инфографики. Благодаря их виральности, результативность повысилась: коэффициент транзакций вырос на 54 %, количество транзакций на 52 %, а доход – на 32 %.

Изменения в рубрикаторе

Чтобы позиционировать маркетплейс как «друга, который знает все», в Facebook-сообществе «Розетки» изменили подход к рубрикам. Их количество сократилось. Появились новые категории, с упором на пользу для клиента:

#нампишуть – публикации самых нелепых и смешных отзывов;

#розеткапитає – рубрика, в которой пользователи голосовали с помощью лайков;

#розеткорисно – ежедневные образовательные и новостные инфографики. связанные с товарной категорией или инфоповодом.

Это сказалось на контенте. Изменение его структуры с января по июль:

– полезный – с 9 % до 43 %;

– развлекательный – с 19 % до 12 %;

– акции и товары – с 72 % до 45 %.

Изменения рубрикатора

Итоги

Facebook-сообщество «Розетка» выросло по всем показателям:

– охват – 231 %;

– количество лайков на 1 пост – 54 %;

– количество комментариев – 352 %;

– вовлеченность – 200 %;

– подписчики – 16 %.

Instagram: фотоконтент и люди

До января «Розетка» в Instagram ориентировалась на интерактив. Этот подход уперся в ограничения – аудитория росла медленно, а основной целью стало ее удержание и поддержание интереса. В Promodo решили изменить ситуацию. Новым вектором стал фотоконтент, производить который помогли штатные фотографы редакции «Розетки».

Instagram развивали отдельно от Facebook. Пересечение контента между ними не должно составлять более 10 %. Особенностью Instagram-аккаунта

сделали открытость, изменив в соответствии тон и содержание коммуникаций. Фокусом стали не технические спецификации, а ответы на «стыдные» вопросы:

– а как это работает?

– а это вообще полезная штука?

– а в этом есть смысл?

– а что это вообще?

– а как оно в жизни выглядит?

В Instagram появилось больше людей, а также новый образ – девушка Маша.

Это сказалось на рубрикаторе и активности. Категория «Лица Розетки» с января по июль прошла путь от появления до статуса одной из самых популярной со средним охватом поста в 23055 взаимодействий. Товарные посты стали «Гаджетами», «Интерактив» сменился на «Fashion», а ситуативный контент просто повысил показатели.

Актуальный рубрикатор «Розетки»

Спецтемы

Чтобы развивать fashion-тематику, привлекли блогера Наташу Шелягину. В рубрике #НаташаСтайл она собирала луки на «Розетке» и показывала в аккаунте. Посты набирали до 4000+ лайков.

Также «Розетка» начала активнее работать со Stories, используя нативные инструменты оформления Instagram. Чтобы выдержать качество публикаций, привлекли сторисмейкера – дизайнера этого формата.

Еще одним нововведением стала рубрика «вопрос – ответ». В ней эксперты отвечали на узкоспециализированные вопросы пользователей. Например, о сборке ПК и подборе компонентов.

Итоги

Instagram-аккаунт «Розетки» количественно вырос. Прирост следующий:

– охват – 72 %;

– лайки на пост – 452 %;

– комментарии на пост – 433 %;

– вовлеченность – 277 %;

– подписчики – 63 %.

Результативность кейса

Общие показатели «Розетки» тоже поднялись. Маркетплейс начал получать из соцсетей на 118 % больше пользователей. Количество транзакций выросло на 152 %, а доход – на 88 %.

(вгору)

Додаток 8

8.11.2018

Ирина Фоменко

Интернет-зависимость ребенка начинается в утробе матери

У детей до 13 лет уже более 1000 фото опубликованы в Интернете, пишет The Telegraph. По словам Комиссара по делам детей Энн Лонгфилд, онлайн-зависимость начинается еще в утробе матери, с того момента, как родители выкладывают УЗИ плода (InternetUA).

Кроме того, дети «растут» в данных, поскольку их личная информация собирается смарт- игрушками, колонками и даже школьными приложениями.

Комиссар обеспокоена по поводу количества личных данных, которые родители и дети публиковали до их 18-летия. Объем информации может иметь серьезные последствия для детей, ведь на решения, которые они должны принимать, влияют алгоритмы.

В докладе Комиссара говорится, в будущем такая информация может повлиять на то, в какие университеты поступят люди, получат ли ипотеку или даже примут ли заявку на работу.

Лонгфилд призвала правительство усилить законы о защите данных для молодых людей и смарт-игрушек, чтобы четко обозначить, хранят ли они информацию о детях.

«Нужно задуматься, что означает для жизни детей сейчас огромное количество данных, и как это может повлиять на их будущее. Мы просто не знаем, каковы будут последствия всей этой информации о наших детях», – заявила Лонгфилд.

В докладе подчеркивается, что в среднем у ребенка около 1300 фотографий и видеороликов, опубликованных в социальных сетях родителями до того, как детям исполнится 13 лет. В возрасте от 11 до 18 лет количество фото вырастает до 70000.

Эксперты отмечают, что родители невольно обнародуют такую ключевую информацию, как имена, возраст и адреса, просто публикуя фотографию своего ребенка в день рождения.

Fashion-журналист Кэтрин Ормерод создала отдельный аккаунт в Instagram, чтобы делиться информацией о материнстве, когда родился ее сын.

«Я всегда думаю о том, что я публикую. Если моему сыну, когда он вырастет, не понравятся фото – я удалю их. Мы всегда должны говорить детям об их цифровых следах, поскольку это будет частью их реальности с самого начала, и у них могут быть разные взгляды на это», – прокомментировала Ормерод.

На сегодняшний день информацию о детях собирают такие устройства, как смарт-колонки и игрушки. Например, CloudPets позволяет родителям записывать сообщения в приложении, которые затем воспроизводятся их ребенку.

Также Комиссар утверждает, что школы и государственные органы собирают огромное количество данных о детях. Например, 70 % школ в Великобритании теперь используют приложение ClassDojo, чтобы отслеживать поведение детей и общаться с родителями.

«Дети часто шокированы, когда узнают, сколько информации о них собирается, пока они растут. Мы должны убедиться, что они понимают, какие данные публикуют», – утверждает Лонгфилд.

(вгору)

Додаток 9

12.11.2018

Эксперимент доказал: социальные сети пагубно влияют на здоровье

Экспериментальное исследование, проведенное психологами из Университета Пенсильвании, впервые показало причинную связь между использованием социальных сетей и более низкими показателями здоровья и самочувствия. В то время как связь между социальными сетями и такими проблемами, как депрессия, беспокойство и одиночество, обсуждались и часто изучались в последние несколько лет, это первый случай, когда исследование показало прямую причинную связь между ними (ITNet).

Психолог Мелисса Г. Хант, заместитель директора центра клинической подготовки по психологии и ее коллеги из Университета Пенсильвании разработали эксперимент по тестированию психологического эффекта, который демонстрировали пользователи, когда им разрешалось использовать социальные сети как обычно или же когда использование ограничивалось до десяти минут на каждую социальную сеть в день.

В начале эксперимента 143 студента прошли опросы, чтобы исследователи могли оценить их здоровье и самочувствие. Затем ученики были разделены на две группы, одной из которых дали полную свободу в использовании привычных социальных сетей, а другую в этом праве ограничили. Участники эксперимента пользовались Facebook, Snapchat и Instagram на протяжении трех недель.

По прошествии трех недель участников снова опросили, используя те же инструменты для измерения их самочувствия. Те, кто свободно пользовались социальными сетями, чувствовали повышенную депрессию, одиночество, беспокойство и страх упустить что-то. Группа студентов, которых ограничили, продемонстрировала значительное снижение беспокойства и страхов, чем было до начала эксперимента.

В частности, люди с более высоким уровнем депрессии в начале исследования показали снижение депрессивных симптомов, когда они сокращали время, проводимое в социальных сетях. Один из них лично рассказал об опыте: «Отсутствие сравнения моей жизни с жизнью других людей оказало гораздо более сильное влияние на меня, чем я ожидал, и в течение этих недель я чувствовал себя гораздо более позитивно в отношении себя».

В то время как самочувствие и использование интернета изучали множество исследований и обнаружили, что, например, у тревожных людей, как правило, есть проблемный подход к использованию интернета или что

депрессия может быть связана с социальными сетями, это первое исследование, подтверждающее это экспериментально. Эксперимент показывает, что не сколько депрессивные, тревожные или несчастные люди чаще используют социальные сети, а скорее, использование данных сайтов снижает самочувствие. Исследователи рекомендуют ограничить использование социальных сетей до 30 минут в день, чтобы улучшить настроение и психическое здоровье.

(вгору)

Додаток 10

7.11.2018
Ирина Фоменко
Основные виды предвыборной дезинформации в соцсетях

Фейковые материалы, вводящие в заблуждение объявления и подозрительные почтовые сообщения являются особенностью большинства современных политических кампаний. Но есть еще одна разновидность дезинформации: непосредственно в день голосования появляются слухи, обман и ложные данные (InternetUA).

The New York Times назвали шесть наиболее распространенных типов дезинформации, а также некоторые советы по их выявлению.

Избирательные пункты

В 2016 году появилось несколько ложных слухов о поведении голосовавших на избирательных участках: утверждалось, что члены участковой избирательной комиссии в штате Невада были одеты в рубашки «Defeat Trump», несмотря на то, что законом это запрещено. На самом деле фото было сделано за несколько дней до выборов.

Еще в одном фейковом материале сообщалось, что агенты иммиграционной и таможенной службы арестовывали голосовавших на выборах. Информация должна была запугать латиноамериканских избирателей.

В ICE заявили, что сотрудники иммиграционной службы не будут патрулировать избирательные участки.

Удаленное голосование

Два года назад граждан вводили в заблуждение – в основном, российские аккаунты – что избиратели могут проголосовать, отправив текстовое сообщение по электронной почте или через Интернет.

Такую информацию могут сновать начать распространять в 2018, и снова она будет ложной: за исключением некоторых избирателей, ни одно государство не разрешает подачу бюллетеней через Интернет, и ни одно правительство не предлагает проголосовать по смс.

Подозрительные сообщения

Текстовые сообщения – это технология кампаний 2018 года, и во многих используются мессенджеры, чтобы побудить избирателей прийти на выборы.

Если вы состоите в партийном комитете, то можете получить сообщения с предложением пойти голосовать и адресом вашего избирательного участка.

Однако будьте осторожны с сообщениями, в которых говорится об изменении часов или места голосования, о требовании новых ID или о недействительности вашей регистрации избирателя. Жители Индианы получали смс якобы от президента Трампа о том, что их голоса не зарегистрированы. В текстах сообщений была ссылка на веб-сайт Национального комитета Республиканской партии, где пользователям предлагалось ввести свои имена, адреса и номера телефонов, а затем предоставить информацию об их избирательных пунктах. Избиратели Джорджии, Канзаса и Мичигана также сообщили о получении аналогичных смс от «Трампа».

Слухи о неисправной работе машины для голосования

Сообщения о сломанных, сфальсифицированных или технически скомпрометированных машинах для голосования могут появиться в день выборов. Могут даже опубликовать видеоролики о неисправности машин. Если у вас нет убедительных доказательств подлинности утверждения, лучше к такой информации относиться скептически.

В 2016 году женщина из Пенсильвании опубликовала вирусное видео на Twitter, в котором утверждалось, что машина для голосования не позволяет ей голосовать за Дональда Трампа. Видео репостнули тысячи раз, и оно вызвало опасения по поводу фальсификации выборов. В любом случае лучше всего принять дополнительные меры предосторожности, несколько раз проверив свой ответ.

Вводящие в заблуждение фотографии и видео

На выборах 2016 года появилось огромное количество доработанных и фейковых фотографий. В этом году ситуация может повториться. Прямо на избирательных пунктах голосующим могут показывать вводящие в заблуждение фото и видео.

Социальные сети пытались бороться с распространением ложной информации о голосовании. Facebook создал «war room» для координации реагирования на подозрительную деятельность в день выборов, а также канал, где чиновники могут отправлять примеры фейковых материалов. Twitter объединился с государственными должностными лицами по выборам и создал портал для обработки отчетов о дезинформации.

Фальсификация результатов выборов

В 2016 Трамп заявил о широкомасштабной фальсификации выборов. Даже после того, как он стал президентом, говорил о миллионах иммигрантов, голосовавших без документов. В действительности такое происходит редко, однако слухи все равно появятся.

В Бразилии, где в прошлом месяце состоялись выборы, в фейковых материалах на Facebook, Twitter и WhatsApp говорилось о фальсификации результатов выборов. Такие действия направлены на подрыв целостности выборов и делегитимизацию победителей.

Рекомендации по проверке дезинформации

По возможности, лучше полагаться на официальные веб-сайты правительства касательно всей информации о голосовании (должно быть .gov в конце адреса веб-сайта). Есть также несколько ресурсов, включая Vote411 и BallotReady, которые предоставляют независимую информацию избирателям.

Прежде, чем сделать репост вирусной истории в день выборов, выглядящей подозрительно, сначала проверьте факты на Snopes или FactCheck.org. Если это фото, выполните поиск изображения с помощью TinEye, чтобы узнать, является ли фотография старой или отредактированной.

Если вы стали свидетелем запугивания избирателей, расскажите об этом работнику избирательной комиссии или по Горячей линии по защите прав избирателей.

(вгору)

Додаток 11

8.11.2018

Российские тролли усиливают активность в социальных сетях

Согласно проведенному исследованию компанией New Knowledge, российская активность в социальных сетях лишь увеличилась, несмотря на комплекс мер, предпринятых США. Осуществленные руководством США меры заставили Россию всего лишь изменить тактику (InternetUA).

Руководители предприятия New Knowledge, которое занимается проблемами кибербезопасности, Райан Фокс и Джонатон Морган сообщили о продолжении Россией реализации своих планов относительно проведения компаний по дезинформации, – сообщает издание The New York Times.

Согласно проведенному исследованию компанией New Knowledge, российские действия по оказанию влияния на американских граждан все еще продолжаются, несмотря на комплекс мер, предпринятых США. Осуществленные руководством США меры заставили Россию всего лишь изменить тактику.

Согласно информации, представленной руководителями New Knowledge, российская активность в социальных сетях лишь увеличилась. За прошлый месяц было выявлено 26 млн постов и 400 пропагандистских сайтов, направленных на американскую аудиторию в целях пропаганды. Среди выявленных сайтов были сайт RT, который содержал 5275 ссылок, сайт The Duran, содержащий 1328 ссылок и сайт Sputnik с количеством 1148 ссылок.

Также были обнаружены аккаунты, действия которых были направлены на оказание влияния на избирателей во время проведения американских промежуточных выборов в Конгресс. Данные посты посвящались убитому диссиденту Джамалю Хашогги, международной политике на Ближнем Востоке и процессу утверждения Бретта Кавано.

Согласно данным, представленным New Knowledge, жертвами российской пропаганды стали миллионы американских граждан.

(вгору)

Додаток 12

4.11.2018

Daily Telegraph рассказала, как Иран и Китай разгромили агентуру ЦРУ с помощью Google

В период с 2009-го по 2013 год ЦРУ США пострадало от «катастрофического» провала, вызванного тем, что иранские власти сумели вскрыть коммуникационную платформу агентства с помощью сервиса Google, пишет The Daily Telegraph. Как отмечает газета, этот промах привёл к ликвидации десятков шпионов в Иране и Китае, с которым Тегеран, по всей видимости, обменялся данными (InternetUA).

Десятки американских шпионов были ликвидированы в Иране и Китае после того, как из-за изъянов в системе коммуникации «враги США за рубежом» с помощью Google смогли узнать, чем они занимаются, пишет The Daily Telegraph.

По данным Yahoo News, в период с 2009-ого по 2013 год ЦРУ США пережило «катастрофический» провал секретных каналов связи на интернет-сайте, который офицеры и полевые агенты по всему миру использовали для разговоров друг с другом.

«Мы до сих пор не преодолели последствия этого события, – отметил один бывший чиновник национальной безопасности. – Из-за этого погибли десятки людей по всему миру».

Коммуникационная интернет-платформа, впервые применённая на Ближнем Востоке для связи с военнослужащими в горячих точках изначально не предназначалась для широкого пользования, однако благодаря простоте в эксплуатации и эффективности её стали использовать различные агенты, хотя та была далека от совершенства.

Дыры в этой платформе стали очевидны только когда Иран, разозлённый тем, что правительство Барака Обамы обнаружило секретную иранскую фабрику ядерного оружия, нашёл отличный инструмент для поиска «кротов».

Тегеран с помощью Google обнаружил один вебсайт, на который заходили американские агенты. Американские чиновники считают, что иранцы сумели воспользоваться этой платформой в качестве поискового инструмента и сумели скрытно выявить секретные сайты ЦРУ.

К 2011 году Иран проник в шпионскую сеть ЦРУ и в мае заявил о ликвидации агентуры США в стране численностью в 30 человек. Некоторых информантов, по словам издания, казнили, другие же оказались в тюрьме.

В то же время 30 агентов, работающих на США в Китае, были казнены правительством, после того как Пекин обнаружил американскую шпионскую сеть с помощью схожих методов. Китаю удалось проникнуть во вторичную коммуникационную систему и обнаружить всех агентов, которые ЦРУ разместил в этой стране.

Источники считают, что Иран и Китай обменялись технической информацией, чтобы атаковать американскую агентуру с двух сторон. В то же время один агент ЦРУ в России получил предупреждение об атаках и сумел сменить канал связи до того, как эта уязвимость нанесла ущерб.

Ещё до инцидента правительство США получило сообщение об уязвимости системы от подрядчика Джона Рейди, который занимался вербовкой источников ЦРУ в Иране. По его донесению, под угрозой провала оказались 70 % операций.

Позднее Рейди уволили по причине «конфликта интересов». По некоторым данным, разведсообщество пришло в ярость, так как, несмотря на тайные слушания этого дела в палате представителей и сенате никто не понёс ответственности за этот провал. Один бывший чиновник по этому поводу заявил, что «самая большая угроза кроется внутри их собственного ведомства».

(вгору)

Додаток 13

5.11.2018

В России хотят создать кибердружины

Депутаты Государственной думы от «Единой России» подготовили законопроект, который предусматривает создание кибердружин. Им надлежит мониторить Интернет и выявлять противоправную и запрещённую информацию. Проект закона представили Адальби Шхагошев, Сергей Боженов, Олег Быков и ряд других народных избранников (Украинский телекоммуникационный портал).

«Кибердружинники, которые в соответствии с этой инициативой смогут выявлять на просторах интернета противоправную информацию, в том числе экстремистского характера, будут теперь законодательно в связи с правоохранительными органами, которые занимаются этим профессионально», – заявил Адальби Шхагошев.

«Это регулирование правового статуса и порядка работы с противоправной информацией, направлен он на гражданскую активность», – уточнил Олег Быков.

Судя по пояснительной записке, кибердружины будут искать данные, направленные на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды. Также в их сферу ответственности попадает запрещённая информация, за распространение которой предусмотрена административная или уголовная ответственность.

Создавать кибердружины планируется в формате общественной организации по инициативе россиян, а принимать туда будут на добровольной основе с 18 лет. О том, как будет оплачиваться такая работа – не сообщается. Зато известно, что прокуратуру, следственные органы, органы государственной власти и местного самоуправления обяжут сотрудничать с кибердружинами.

Это уже далеко не первая инициатива законодателей по контролю Интернета. Ранее депутат от КПРФ и председатель комитета Госдумы по вопросам семьи, женщин и детей Тамара Плетнёва заявила о необходимости запретить сайты и приложения для знакомства.

Также отметим, что кибердружины уже есть во многих местах, однако они работают разрозненно и зачастую неофициально. Новый проект закона должен, как ожидается, должен улучшить их работу.

(вгору)

Додаток 14

12.11.2018

У Франції податкова буде моніторити сторінки неплатників податків у соцмережах // Фото з розкішними авто або на узбережжі Маямі викличуть підозру, чи справді людина така бідна, як прикидається

Якщо громадянин Франції не сплачує податки, але постить у соцмережах фото з розкішними будинками чи автомобілями – він тепер стане об'єктом прискіпливої уваги податкових інспекторів, пише hightech.plus з посиланням на заяву міністра держслужби і держбюджету Франції Жеральда Дарманена (Mind).

З 2019 року Франція прирівняє публікації в соцмережах до доказів – і підключить до їх пошуку штучний інтелект.

З початку 2019 року податкові інспектори у Франції почнуть моніторити публікації в соціальних мережах для пошуку порушників. Проект запустять в пілотному режимі нарівні з іншими заходами щодо боротьби зі злісними неплатниками.

Інспекція буде зіставляти реальні доходи громадян з публікаціями в соцмережах.

«Якщо ви постійно фотографуєте з розкішним автомобілем, але коштів на таку покупку у вас немає, то, можливо, машину вам позичив двоюрідний брат чи дівчина. А може, й ні», – зауважив Дарманен в інтерв'ю телеканалу M6.

Пости в соцмережах можуть викликати підозри в ухиленні від сплати податків і стати причиною для розслідування, попередив чиновник.

Поки що для пошуку порушників податкова служба Франції моніторить оголошення про покупку і продаж. Багато операцій інспектори проводять вручну, але з 2019 року влада планує впровадити алгоритм для збору і аналізу великих даних.

Видання Connexion пояснює, що система буде виявляти підозрілі випадки, які потім оцінять дата-фахівці. Тільки після цього інформацію передадуть співробітникам податкової служби.

Інші країни також використовують дані соцмереж для пошуку податкових шахраїв. Однак такі програми відкрито не афішуються. У 2013 році в США широко висвітлювали випадок Рашиї Вілсон, яка публікувала на своїй сторінці в Facebook фотографії з пачками грошей і називала себе «королевою

податкового шахрайства». Пізніше її пости стали доказами в суді, а Вілсон засудили до 21 року ув'язнення.

Між тим, згідно зі статистикою, органи Державної фіскальної служби України провели протягом 2018 року 18 542 судів з українським бізнесом та громадянами.

(вгору)

Додаток 15

31.10.2018

Против «ВКонтакте» подали первый иск за разглашение правоохранителям персональных данных

Сотрудница штаба российского оппозиционера Алексея Навального Лилия Чанышева подала иск в суд Санкт-Петербурга на администрацию социальной сети «ВКонтакте» за разглашение правоохранительным органам личной информации пользователей. Об этом говорится в сообщении, опубликованном на официальном сайте Алексея Навального (InternetUA).

«30 октября сотрудник штаба Навального в Уфе Лилия Чанышева обратилась в Смольнинский суд Санкт-Петербурга: она подала иск к "ВКонтакте" и требует признать действия администрации соцсети незаконными, а также присудить ей компенсацию в размере 100 тысяч рублей», – говорится в сообщении.

По словам юриста правозащитной группы «Агора» Дамира Гайнутдинова, когда правоохранители запрашивали у администрации «ВКонтакте» личные данные Чанышевой, то обосновали правомерность своих действий, сославшись на российские законы «О полиции» и «Об оперативно-розыскной деятельности». Но, как отметил Гайнутдинов, этого не достаточно для получения личной информации пользователя.

«Основная цель – привлечь "ВКонтакте" к ответственности, чтобы остудить пыл этой соцсети в части незаконного слива личной информации и частной переписки как в отношении меня, так и в отношении других пользователей в будущем», – заявила сама Чанышева в разговоре с российским медиа «Проект».

В иске против «ВКонтакте» говорится о том, что указанные законы разрешают правоохранителям собирать данные о россиянах «исключительно в пределах своих полномочий» и «в связи с расследуемыми уголовными делами и находящимися в производстве делами об административных правонарушениях, а также в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях».

Отмечено, что есть случаи, когда «Вконтакте» раскрывал личные данные сотрудникам ФСБ и МВД РФ по запросу, который просто прислали по электронной почте. Причем в последние несколько месяцев вызвали в России

общественный резонанс те случаи, когда полиция возбуждала уголовные дела из-за постов в соцсети.

При этом официальные представители «ВКонтакте» говорят о своей приверженности защите персональных данных пользователей и заявляют о том, что подобную информацию выдают полиции только в рамках закона.

Как сообщалось ранее, жительница Барнаула Мария Мотузная, которую в России судят за публикацию картинок во «ВКонтакте», рассказала, что администрация соцсети предоставила следователям данные об IP-адресах, с которых заходили на страницу, изменения паролей, изменения прикрепленного номера телефона, имени и фамилии пользователя. Кроме того, в материалах есть сведения об обращении в службу поддержки соцсети и блокировки страницы за спам.

(вгору)

Додаток 16

31.10.2018

Google удалила из Google Play 29 банковских троянов

Эксперт антивирусной компании ESET Лукас Стефанко узнал о существовании 29 вредоносных приложений для Android, которым удалось обойти защиту Google Play и закрепиться в каталоге. Все они были ориентированы на кражу учетных данных для доступа к банковским счетам своих жертв. Для этого программы провоцировали появление на экранах зараженных устройств поддельные окна авторизации, имитирующие начальные страницы популярных онлайн-банков (InternetUA).

Дабы охватить максимально широкую аудиторию, мошенники прятали вредоносный код в приложения самого разного толка. В числе инфицированного ПО попадались всевозможные каталоги гороскопов, бустеры, утилиты для чистки памяти и другие пользующиеся спросом программы. Такая стратегия дала свои плоды и всего за пару месяцев троян удалось распространить по меньшей мере среди 30 тысяч пользователей устройств на Android.

Банковские трояны для Android

– Astro Plus
– Power Manager
– Master Cleaner – CPU Booster
– Master Cleanser – Power Booster
– Super Boost Cleaner
– Super Fast Cleanet
– Daily Horoscope For All Zodiac Signs
– Daily Horoscope Free – Horoscope Compability
– Phone Booster – CPU Cooker
– Ultra Phone Booster
– Free Daily Horoscope 2019

– Free Daily Horoscope Plus – Astrology Online
– Phone Power Booster
– Ultra Cleaner – Power Boost
– Master Cleaner – CPU Booster
– Daily Horoscope – Astrological Forecast
– Speed Cleaner – CPU Cooler
– Horoscope 2018
– Meu Horoscopo
– Master Clean – Power Booster
– Boost Your Phone
– Phone Cleaner – Booster, Optimizer
– Clean Master Pro
– Clean Master – Booster Pro
– BoostFX
– Personal Horoscope

Поведение банковских троянов

В отличие от большинства троянов, мимикрирующих под легитимное ПО для доступа к банковским счетам, эти до последнего ведут себя максимально неприметно. Попадая на устройства своих жертв, многие приложения сообщали о несовместимости и скрывались с рабочего стола, имитируя самоудаление, после чего начинали сканировать память на предмет установленных банковских клиентов, в зависимости от которых троян формировал поддельную страницу авторизации.

На момент выхода публикации все вредоносные приложения из списка удалены из Google Play.

(вгору)

Додаток 17

31.10.2018

Михаил Сапитон

Десктопный клиент Telegram хранит переписку в незащищенном виде. Это не компрометирует мессенджер

Первокурсник американского колледжа Wake Technical Натаниэль Сачи публично раскритиковал защищенный мессенджер Telegram. Он обнаружил, что программа хранит содержимое чатов локально, в незащищенном виде и пожаловался на ситуацию в Twitter (AIN.UA).

Дело касается клиента Telegram Desktop – единого приложения под Windows, macOS и Linux (также у мессенджера есть нативный клиент для macOS). О работе Сачи написало издание Bleepingcomputer.

Переписка находится в базе данных, расположенной в одной из папок программы. Прочитать SQLite-файл непросто, однако при помощи скриптов и некоторой подготовки, возможно. По наблюдениям Сачи, туда попадают не только сообщения, но и номера телефонов, а также названия контактов.

Протестировав функцию секретных чатов, при которых данные передаются по принципу end-to-end и не хранятся на серверах, исследователь также якобы обнаружил в базе данных содержимое переписки. Этот пункт вызывает вопросы – в Telegram Desktop нет поддержки секретных чатов. Они работают в нативном клиенте для macOS и на мобильных устройствах.

Особенно Сачи побеспокоило, что Telegram Desktop предлагает закрыть доступ к приложению паролем. Даже если эта мера остановит посторонних от прямого чтения чатов, они могут беспрепятственно скопировать базу данных. Студент заключает, что это создает иллюзию защищенности среди рядовых пользователей.

Telegram – не первый мессенджер, который подвергся подобным обвинениями. Ранее француз Натаниэль Сюиш высказал аналогичные претензии к Signal. Программа хранила переписку в виде JSON-файлов, открытых для чтения.

Почему это не проблема

Оба случая не компрометируют мессенджеры. И Telegram, и Signal ручаются лишь за безопасность своих протоколов передачи данных. Защита устройств от постороннего доступа остается за пользователем. Это признает и сам Сачи, отмечая вклад Signal и Telegram в улучшение онлайн-безопасности. Он указывает, что у его работы просветительская цель. Защищенные мессенджеры часто используют активисты и, при завышенных ожиданиях от безопасности, могут поставить свою жизнь под угрозу.

Ситуацию вокруг Telegram осветили СМИ. В публикациях Сачи часто называли «экспертом по кибербезопасности», а хранение незащищенных файлов – уязвимостью. Ажиотаж вызвал реакцию Павла Дурова, основателя Telegram. В своем канале предприниматель написал:

– С технической точки зрения утверждение заявившего об уязвимости сводится к следующему: «Если бы у меня был доступ к Вашему компьютеру, я бы смог прочитать Ваши сообщения».

Само по себе это утверждение очевидно, но его завуалированное описание позволяет запутать человека, далекого от технологий. Три года назад я рассказывал о похожем случае.

Случай, о котором упоминает Дуров – разбор заявления о том, что защиту Telegram на Android можно обойти, получив Root-доступ к устройству. Тогда основатель Telegram объяснял, почему ключи для расшифровки переписки в локальной базе данных хранятся на устройстве. Если бы они отсутствовали, программа не смогла бы даже отобразить сообщения. Дуров подчеркивал, что при получении контроля над устройством, винить мессенджер в небезопасном хранении данных – спекуляция.

(вгору)

Додаток 18

31.10.2018

В Швеции тысячи людей вживили себе под кожу упрощающие жизнь чипы

В Швеции наблюдается повальное увлечение биохакингом. Тысячи граждан вживили себе под кожу чипы, в которых хранится личная информация и с помощью которых можно взаимодействовать с окружающей технологической средой (например, платить в магазинах). Тенденция пока не планирует сбавлять обороты, но некоторые учёные говорят, что массовое вживление чипов таит в себе ряд опасностей (InternetUA).

В 2017 году шведская компания Epicenter одной из первых в мире вживила своим сотрудникам под кожу маленькие чипы, которые служат пропуском, дают доступ к офисной технике и позволяют расплачиваться в местном кафе. То же самое сделала и одна из американских фирм, говоря, что рано или поздно так начнут делать все. И этот прогноз начал сбываться, как минимум для Швеции.

В стране сейчас наблюдается повальное увлечение чипированием. Люди вживляют себе под кожу чипы, размером с рисовое зерно, и уверяют, что они значительно облегчают жизнь.

По словам одной из компаний Biohax, занимающихся вживление чипов, только через них уже прошли четыре тысячи клиентов, пишет Independent.

Подкожные чипы, которые вводятся под кожу между большим и указательным пальцами, используют технологию радиочастотной идентификации (RFID). В них можно зашить любую информацию – от данных паспорта до кредитной карты. Чипы могут быть прочитаны любым устройством, поддерживающим технологию NFC), то есть, большинство современных смартфонов Android могут их распознать. Они не нуждаются в подзарядке, так как они не требуют использования батареи.

С помощью чипов можно попасть в офис, расплатиться в магазине, а также использовать их как хранилище для документов. Люди, вживившие их, уверяют, что стало гораздо проще и быстрее совершать повседневные действия вроде покупок или прохождение контроля в аэропорту. Сами производители чипов говорят, что они также помогают миру снизить количество пластиковых отходов, так как банкам теперь не нужно выпускать тысячи кредиток.

В последние годы нам удалось договориться с нескольким корпорациям, чтобы обменять их пластиковые карты доступа на установку Biohax, – говорят в компании. – Также мы добились того, чтобы шведской национальной железнодорожной системе разрешить использование Biohax в качестве замены бумажных билетов и пластиковых проездных карточек.

Есть несколько причин, по которым чипирование в Швеции стало массовым явлением, пишет NPR. Во-первых, в стране технологический прогресс с 90-х годов поддерживается правительством, вплоть до того, что компаниям, покупавшим сотрудникам домашние компьютеры, давали налоговые льготы. Во-вторых, в стране распространены безналичные платежи. Только один из четырёх шведов использует наличные. Ну и наконец, в Швеции

немного проще, чем в других странах, относятся к персональным данным. Граждане привыкли предоставлять их во время онлайн-покупок или административным органам.

Некоторые эксперты считают, что в последнем пункте таится опасность для массового использовании чипов. В частности речь идёт о безопасности конфиденциальных данных, которые хранятся в чипах. Ведь получается, что люди носят при себе полный комплект документов и данные кредитных карт.

Среди скептиков – микробиолог Бен Либбертон, британский учёный, базирующийся в южной Швеции. Он входит в число тех, кто начинает кампанию за то, чтобы чипирование начало как–то контролироваться законодательно.

То, что происходит сейчас, относительно безопасно, но если оно используется повсеместно, если каждый раз, когда вы хотите что-то сделать, и вместо использования карты вы используете свой чип, может быть очень и очень легко раскрыть личную информацию.

Но несмотря на опасения, тенденция пока не снижается. Более того, в продажу поступили новые чипы с увеличенным объёмом памяти и рядом новых функций. Например, чипы теперь начнут мигать красным цветом, если кт-–то посторонний попытается получить с них информацию.

В отличие от Швеции, в других странах, люди, вживившие чипы, могут столкнуться с проблемами. Так в Австралии биохакер по имени киборг Мяу-Мяу, прошёл в метро просто приложив к сканеру руку. Но служба безопасности не поняла, что произошло.

Кроме того, биохакинг может решить далеко не все человеческие проблемы, например, не поможет найти девушку. Биохакер из США так отчаялся, что даже предложил большие деньги тому, кто поможет ему найти вторую половинку. Правда, список требований к спутнице у него получился такой, что начинаешь подозревать, в чём причина его одиночества.

(вгору)

Додаток 19

1.11.2018

Dell EMC Cyber Recovery обеспечит последнюю линию защиты данных от кибератак

Компания Dell EMC представляет ПО Cyber Recovery и сервисы для восстановления и реабилитации, которые помогут обеспечить последнюю линию защиты данных от кибератак и программ-вымогателей. Новое ПО включает инструменты для автоматизации, рабочих загрузок и анализа состояния безопасности, которые обеспечивают защиту и изоляцию критически важных данных уровня «золотых» копий, с тем чтобы после отражения атаки в максимально сжатые сроки восстановить бизнес-процессы (Компьютерное Обозрение).

Dell EMC Cyber Recovery интегрируется с аппаратным обеспечением хранилищ Data Domain. Оно автоматизирует сохранение изолированных защищенных копий критически важных данных внутри хранилища Cyber Recovery Vault (CR Vault), убирая их с атакуемой поверхности.

Используя хранилище CR Vault пользователи могут проанализировать состояние защиты сохраненных данных, не прибегая при этом к необходимости восстанавливать и активировать вредоносное ПО, которое могло бы оказаться в защищенном наборе данных.

Новый фреймворк автоматизации тестирования REST API обеспечивает беспрепятственную (seamless) интеграцию с пакетом ПО для аналитики безопасности – Index Engines CyberSense, которое применяет более 40 эвристик для обнаружения угрозы.

Кроме того, Dell EMC предлагает комплекс услуг Cyber Recovery Services для персонализированного усиления защиты и безопасности. Он включает воркшоп, консультации, услуги развертывания и внедрения.

ПО Dell EMC Cyber Recovery уже доступно в мире без дополнительной платы при покупке систем хранения Dell EMC Data Domain (DDOS 6.0.x и выше). Соответствующие сервисы также уже доступны заказчикам.

(вгору)

Додаток 20

2.11.2018

Рекламное ПО и майнеры лидируют в октябрьском рейтинге вирусов

Компания Eset представила тенденции распространения компьютерных угроз в октябре. Согласно данным, полученным с помощью системы быстрого оповещения Eset LiveGrid, топовые позиции в рейтинге наиболее активных вредоносных программ занимает рекламное ПО и угрозы для скрытой добычи криптовалюты (Компьютерное Обозрение).

В частности, наибольший уровень распространения в Украине (9.17 %) и мире (21.93 %) на протяжении месяца продемонстрировал зловред JS/Adware.Agent.AA, который предназначен для показа рекламных сообщений. Подобные возможности имеет и угроза Win64/Adware.PBot (1.25 %). Как правило, после проникновения на компьютер жертвы такие вирусы показывают рекламные баннеры, всплывающие сообщения, а также могут устанавливать дополнительные программы, которые содержат рекламу.

Вторую позицию в украинском рейтинге удерживает угроза SMB/Exploit.DoublePulsar (8.44 %), которая предотвращает использование уязвимых систем вредоносным ПО Win32/Exploit.CVE–2017–0147.A и Win32/Filecoder.WannaCryptor.

Замыкает тройку самых активных программ угроза JS/CoinMiner (4.9 %), которая использует аппаратные ресурсы зараженного компьютера для скрытой добычи криптовалюты. В топ-10 также вошли такие угрозы для скрытой

добычи криптовалюты, как Win32/CoinMiner (2.42 %) и Win64/CoinMiner (1.65 %).

Кроме этого, активным оставался HTML/ScrInject (2.7 %). Угроза перенаправляет пользователей на ресурсы с вредоносным ПО, а ее код, как правило, встроен в HTML-страницы.

Одну из последних позиций заняла угроза Android/Hiddad, которая нацелена на мобильные устройства. Троянская программа выдает себя за приложение для загрузки видео с YouTube. После получения прав администратора приложение начинает отображать рекламу и требует поставить ему 5 звезд в магазине GooglePlay.

(вгору)

Додаток 21

2.11.2018

Google придумала новый способ борьбы с вирусами на Android

Разработчики «Корпорации добра» начали испытания новой системы защиты пользователей, которая активируется при попытке входа в учетную запись Google. Об этом говорится в официальном блоге поискового гиганта. Нововведение предусматривает задействование JavaScript для сканирования устройства на предмет вредоносных компонентов, препятствуя авторизации во избежание кражи учетных данных мошенниками с целью последующей компрометации аккаунта и его использования в личных целях (InternetUA).

Отныне всякий раз при входе на страницу авторизации, объясняют разработчики, будет выполняться оценка риска. В случае обнаружения на устройстве вредоносного или другого подозрительного ПО, система запретит авторизацию до момента очистки памяти. А чтобы пользователю было легче справиться с задачей, специальные алгоритмы укажут на конкретные приложения, которые подрывают безопасность устройства и тем самым препятствуют входу в учетную запись.

Чтобы проверка состоялась, необходимо, чтобы на устройстве не была отключена работа JavaScript. Несмотря на то что у подавляющего большинства пользователей данная надстройка включена по умолчанию, некоторые предпочитают отключать ее. В этом случае потребуется активировать JavaScript, перейдя в настройки JavaScript в конфигурациях своего браузера и передвинув ползунок активации в положение «вкл.». Так вы будете уверены, что безопасности вашей учетной записи ничто не угрожает.

В случае, если ваша учетная запись была скомпрометирована ранее, алгоритмы Google поймут это и предложат оценить нанесенный ущерб и способы возвращения контроля. При желании вы всегда можете самостоятельно проверить, какие приложения и сервисы имеют доступ к вашей учетной записи. Для этого перейдите в раздел безопасности, где представлен полный перечень ПО, которому разрешен доступ к вашей информации, сохраненной на серверах Google.

(вгору)

Додаток 22

2.11.2018

Українець розсилав комп'ютерний вірус під виглядом розважальних програм

Працівники Причорноморського управління Департаменту кіберполіції викрили мешканця Миколаєва у розповсюдженні шкідливого програмного забезпечення (InternetUA).

Завдяки модифікації вірусу зловмисник дистанційно керував комп'ютером жертви, а також отримував доступ до веб-камери інфікованого комп'ютера. Вирішується питання щодо оголошення йому підозри за двома статтями Кримінального кодексу України.

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) КК України.

Під час обшуку у квартирі зловмисника поліцейські вилучили ноутбук, де знаходилась адміністративна панель керування шкідливим програмним засобом.

Крім того, працівники кіберполіції встановили, що зловмисник з метою розповсюдження шкідливого програмного засобу створив декілька каналів на відеохостінгу «Youtube». На цих каналах він розміщував відеорекламу розважальних програм для комп'ютера, та у опису до відео надавав посилання, через яке користувач мав можливість завантажити таку програму. Натомість користувач завантажував шкідливе програмне забезпечення.

Під час попереднього огляду вилученої техніки встановлено близько 50 комп'ютерів, уражених шкідливим програмним засобом. Також, виявлено інформацію, яку зловмисник встиг скопіювати з комп'ютерів жертв.

Наразі вилучену техніку направлено на проведення комп'ютерно-технічної експертизи. Вирішується питання щодо оголошення підозри хакеру за ч. 2 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

(вгору)

Додаток 23

4.11.2018

На промышленных USB-накопителях обнаружены опасные вирусы

USB-накопители представляют серьезную угрозу промышленным системам и могут использоваться для вмешательства в работу сервисов энергетических компаний, предприятий коммунального водоснабжения и других организаций в сфере критической инфраструктуры. К такому выводу пришли специалисты компании Honeywell по итогам исследования потенциальных рисков, представляемых использованием USB-накопителей (InternetUA).

Специалисты проанализировали данные, собранные от 50 организаций в США, Южной Америке, Европе и на Среднем Востоке, и выяснили, что 44 % «флешек», применяемых на промышленных предприятиях, содержали по меньшей мере один небезопасный файл. В общей сложности 26 % выявленных угроз обладали потенциалом вызывать операционные проблемы, включая потерю операторами контроля над системой.

Наиболее распространенным типом вредоносного ПО, обнаруженного на зараженных «флешках», оказались трояны с различным функционалом, в том числе способностью создавать бэкдоры, красть конфиденциальную информацию или загружать дополнительные вредоносные модули через управляющий сервер. Исследователи также выявили дропперы, хакерские инструменты и потенциально нежелательные программы.

Согласно докладу, 2 % инфицированных накопителей содержали вредоносное ПО Triton, применявшееся в атаках на системы безопасности Schneider Electric Triconex. На 6 % устройств был обнаружен вредонос Mirai, 2 % накопителей были инфицированы печальноизвестным червем Stuxnet, использовавшимся в атаках на ядерные объекты в Иране в 2010 году, а 1 % устройств содержал вредоносное ПО WannaCry.

«Данное исследование подтверждает то, что мы подозревали в течение многих лет – USB-накопители представляют реальную угрозу для промышленных операторов. Неожиданностью стал масштаб и серьезность угроз, большинство из которых могут привести к возникновению опасных ситуаций на площадках, где осуществляются производственные процессы», – указывается в отчете.

(вгору)

Додаток 24

5.11.2018

Американські вчені розробили дієву програму для боротьби із кібершахраями

За допомогою нової програми дослідники допомагають правоохоронним органам боротися з шахраями, які крадуть дані електронних поштових скриньок (Espreso.tv).

Як пише Eurek Alert, новий інструмент візуальної аналітики значно прискорює досудові розслідування і виділяє критичні посилання.

Правоохоронним органам часто не вистачає ресурсів для ідентифікації кіберзлочинців, які продовжують активну діяльність щодо електронного листування користувачів.

Для вирішення питання дослідницька група з Нью-Йоркського університету разом з компанією Agari розробила програму «Бігль» (Beagle) – візуальний аналітичний інтерфейс, який може працювати з безліччю листів, підсумовувати дані з них, виділяти загальні риси.

Вчені наголосили, що програма добре систематизує дані, які правоохоронці часто не помічають – час відправлення листа, місце розташування жертв, ключові слова та шаблони шахраїв.

«Ділова електронна пошта всю історію була пов'язана з різними формами шахрайства в дрібному і більш глобальному масштабі», – відзначили дослідники. «Бігль» розширив наші можливості з моніторингу та відстеження цих злочинних організацій, відобразивши більш повну картину залучених осіб та їх взаємин один з одним».

Програму тестували на реальній справі, де було потрібно знайти мережу шахраїв і жертв, спираючись тільки на десяток скомпрометованих листів. «Бігль» зміг візуалізувати це, а потім передати дані з відображеними зв'язками правоохоронним органам.

«Ми були здивовані, виявивши, що програма дійсно може зібрати докази, які можна використовувати для кримінального процесу», – зазначили вчені, додавши, що інструмент може посилити аналітичний процес, виявивши зв'язки, які призводять до збільшення бази даних слідчих.

(вгору)

Додаток 25

5.11.2018

Ирина Фоменко

Боты обманывают покупателей на деньги, используя их персональные данные

Великобритания начинает расследование использования персональных данных для установления индивидуальных цен на праздники, автомобили и товары для дома в связи с растущими опасениями об обмане потребителей. Об этом сообщает The Guardian (InternetUA).

Согласно исследованию органа контроля за соблюдением законодательства о защите экономической конкуренции, эксперты изучат распространенность «динамического ценообразования» на основе информации, собранной о человеке, такой как геолокация, семейное положение, дата рождения или история поездок.

По данным Управления национальной статистики, возникают опасения по поводу использования технологий, в том числе искусственного интеллекта и ботов, для «персонализации» цен в ущерб некоторым покупателям.

Цены на онлайн-слуги колеблются в зависимости от времени суток или доступности – будь то билеты или такси Uber. Теперь в магазинах начали появляться цифровые этикетки, где цены устанавливаются в зависимости от спроса.

«Важно понимать, как достижения в области технологий влияют на потребителей. Нужно знать, как лучше всего защитить людей от обмана. Мы также будем использовать результаты наших постоянных усилий, чтобы помогать уязвимым потребителям», – заявил исполнительный директор Competition and Markets Authority (CMA) Андреа Косчелли.

Этот вопрос обсуждался на прошлой неделе на форуме, в котором приняли участие CMA, Ofcom, Ofgem и Управление гражданской авиации. Канцлер Филип Хэммонд попросил группу экспертов, возглавляемую Джейсоном Фурманом, бывшим советником Барака Обамы, изучить конкуренцию в цифровой экономике, в том числе и то, как машинное обучение и алгоритмы используются для установления цен и могут ли фирмы сговориться для обмана потребителей.

«Британские компании лидируют в освоении новых технологий. Но они не должны злоупотреблять этими технологиями и данными в ущерб потребителям», – прокомментировал бизнес–секретарь Грег Кларк.

(вгору)

Додаток 26

5.11.2018

В Стэнфорде изобрели надежный метод шифрования персональных данных

Все пользователи сталкиваются с тем, что программа или устройство запрашивает разрешение на отправку данных разработчикам. Запрет этого действия на самом деле неэффективен – в ПО часто встроены механизмы передачи информации разработчику. В Стэнфордском университете (США) придумали способ шифрования персональных данных, обеспечивающий практически 100-процентную защиту (InternetUA).

Стэнфордские специалисты создали алгоритм, который агрегирует все отчеты об использовании любой компьютеризированной системы. При этом основной упор делается на защиту персональных данных. Вся персональная информация шифруется по методу, известному как «разделение секрета», сообщается на сайте университета.

«В нашей жизни все больше электроники, которая собирает личные данные и отправляют их производителю. Это лампочки, автомобили, тостеры… Рост числа этих устройств означает, что все больше конфиденциальных данных пользователя утекает от него», – говорит один из авторов защищающего данные ПО Генри Корриган-Гиббс.

Принцип работы алгоритма заключается в том, чтобы разрешить производителям собирать исключительно техническую информацию, но гарантированно защитить важные для пользователя факты и цифры.

Все приватные данные шифруются и делятся на части. В таком распределении и состоит главная особенность метода криптографии «разделение секрета». В случае, если недобросовестный разработчик решит заполучить ваши персональные данные, он получит лишь зашифрованный набор части эти данных, который без наличия других частей не предоставляет никакой ценности.

Система стэнфордских специалистов называется Prio и уже тестируется в браузере от Mozila.

С тем, что неконтролируемый сбор данных – одна из главных проблем современного интернета согласен глава Apple Тим Кук. «Сбор персональных данных – это оружие, направленное против всех нас», – говорит он. Кук призвал ограничить ИТ-гигантов в праве собирать персональные данные пользователей и торговать ими.

(вгору)

Додаток 27

6.11.2018

Обережно, за вами слідкують: як онлайн-технології шпигують за людьми

Мобільний телефон знає про вас все. Які дані збирають про користувачів Facebook, Google та мобільні додатки, чи прослуховують оператори ваші дзвінки та поради, як захистити свою інформацію (InternetUA)?

Нещодавно стало відомо, що інформацію про 257 тисяч користувачів Facebook виклали у вільний доступ. Хоча хакери стверджують, що мають дані 120 млн осіб.

Facebook знає все про своїх користувачів. Соціальна мережа збирає 98 видів інформації – від геолокації, до рівня освіти, доходу, кількості кредитних карт та переваг у одязі. Такі дані опублікувало видання Washington Post у 2016 році.

Основне джерело інформації – мобільний телефон. Як мінімум тому, що ви завжди носите його з собою і користуєтесь для виходу в інтернет.

Українці в середньому проводять 4 години в день у своєму телефоні. Про це свідчать дослідження Mastercard.

Смартфон став своєрідним пристроєм спостереження XXI сторіччя, а користувачі свідомо дозволяють відстежувати кожен свій крок.

Як і навіщо пристрої збирають персональні дані та чи можна їх захистити, розповів Артем Верещака Senior Software Engineer у компанії Taxify.

Навіщо інтернету ваші дані?

Вам приходили повідомлення про знижки в магазині, як тільки ви зайшли в торговий центр? Або вспливала реклама закладу, коли ви знаходились поруч?

Це не збіг обставин. Просто телефон передає дані про ваші переміщення, а тому реклама приходить у відповідний момент.

– За допомогою цієї інформації (персональних даних, – Ред.) можна зробити рекламу більш ефективною, можна передбачити, що вам знадобиться в майбутньому, можна аналізувати поведінку користувачів і покращувати сервіс.

З одного боку, ми не можемо відчувати себе захищеними, а з іншого – такі речі спрощують нам життя.

– Геолокація, історія серфінгу в інтернеті, історія покупок, історія переглядів фільмів і все це накладено на час. Зібравши навіть малу частину відкритої інформації про людину, можна досить детально відстежити історію її переміщень, скільки вона витрачає часу на обід, де це робить і що замовляє.

Безкоштовні додатки заробляють на вас

Чому додатки, якими ми користуємось, безкоштовні? Очевидно, що більшість заробляють на рекламі. Однак, існують безкоштовні додатки без реклами. І користуються вони, як правило, більшою популярністю.

Використовуючи такі додатки слід насторожитись – скоріш за все вони збирають ваші особисті дані:

– Всі ці «безкоштовні» сервіси, такі як VPN-сервіс, Facebook, Vk, Google Mail, Google Calendar, Google Photos не є безкоштовними. Хто розробляв би такі сервіси за величезні суми грошей, підтримував їх, оплачував сервера, електрику просто так? Ви платите велику ціну – особисті дані.

Встановлюючи додатки на телефон, часто людина навіть не читає умови користування. Так вона надає доступ до своєї інформації. І велику долю інформації збирають як раз VPN сервісі, які набули популярності після блокування в Україні низки російських сайтів.

– Що є VPN-сервіс? Грубо кажучи, це проксі, тобто прошарок, між вами і тим, куди ви хочете потрапити. Припустимо, ви хочете отримувати доступ до Vk, але він заблокований в Україні. Тому з VPN-сервісом ваш запит йде спочатку кудись в Нідерланди, там він запитує дані від серверів Vk, потім відповідає вам.

В принципі виглядає доволі безпечно. Враховуючи, що програма дозволяє вам користуватись улюбленою соціальною мережею. Тим паче безкоштовно. Але і тут є свої підводні камені:

– Будь-який безкоштовний VPN-сервіс не буде працювати на доброму слові. Вони зберігають всі ваші запити, знають куди і навіщо ви заходите (адже ви зареєструвались і вказали свої дані). Хороший VPN-сервіс буде платним. Так можна сподіватися, що ваші дані швидко зникають з їх серверів.

Надалі подібні програми продають ваші персональні дані рекламним майданчикам за колосальні суми.

Нещодавно з’явився чудовий додаток GetContact, який дозволяє дізнатись, як ви підписані у своїх друзів. Начебто нічого особливого, лише чергова розвага.

Але компанія-розробник непогано заробила, збираючи з вашого дозволу інформацію про ваші контакти, а потім продаючи бази даних мобільних

номерів третім особам. Саме в такий спосіб сервіси таксі, якими ви ніколи не користувались, присилають вам смс про знижки.

Facebook впливає на ваш вибір

Чим більше часу ви проводите у Facebook, тим більше інформації він на вас збирає. Ці дані він продає своїм рекламодавцям. Тому ви можете бачити одну рекламу, а ваш знайомий – іншу.

– Facebook знає про вас дуже багато. Навіть те, на скільки ви затримались у стрічці, щоб щось прочитати, не кажучи вже про перехід за посиланням, лайки, спілкування, геолокацію та ін.

На початку 2018 року у світовій спільноті вибухнув скандал з Facebook. Мова йшла про найбільший витік даних за всю історію компанії – інформація про 50 млн користувачів. Ці дані потрапили в аналітичну компанію, яка використала їх для політичної пропаганди під час виборів президента США.

– Зараз ви можете подивитись, що у Facebook на вас є (а там дуже багато, я запевняю). В налаштуваннях досить глибоко і дрібним текстом заховане посилання, де можна вивантажити архів з даними, які Facebook зберігає про вас.

Збираючи і обробляючи інформацію про вас, Facebook допомагає вам читати відповідні новини, вибирати лідера країни, формувати цінності та переконання і навіть витрачати ваші гроші. На жаль, не зажди ефективно:

– Аналіз даних і психологія здатна змусити людей робити багато чого. Таким чином вам продають непотрібні товари, змушують щороку міняти смартфон на новий і більш «прогресивний».

Google знає про вас все

Google певне збирає найбільші масиви інформації про своїх користувачів. А користуються його послугами всі:

– Google володіє багатьма зручними сервісами і власною ОС – Android. Вони збирають великі і комплексні масиви даних – ви ж використовуєте Chrome, Calendar, GMail, Google Фото, Google Keep, Google Pay та ін. У їх розпорядженні ваші плани, покупки, історія спілкування, історія браузера, історія пересувань (дуже точна).

Однак, все це Google робить з вашого дозволу. Ці сервіси і послуги в якомусь сенсі покращують життя:

– Google Фото відсортує ваші знімки в альбоми по датах, локаціях або навіть людях на фото.

– Youtube (він також належить Google) порекомендує цікаві відео.

– GMail автоматично створить нагадування про візит до дантиста.

– Google Maps може в якийсь момент сказати вам, що поруч є непогані заклади з тайської їжею, тому що він знає, що вам подобаються такі.

– Google Pay не змусить ще раз вводити дані платіжної карти, адже він запам’ятав їх в минулий раз.

Таким чином в інтернеті не залишається місця для конфіденційності:

– Google аналізує кожен лист. Інакше, як він вам підказує, що можна відповісти або пропонує винести подію в календар і створити нагадування?

Для того, щоб переконатись у тому, що за вами слідкують, просто перейдіть в Google Timeline (вбийте в пошук і перейдіть за першим) і знайдете досить точну історію ваших переміщень.

Мобільні оператори

Чи можна розраховувати на конфіденційність з мобільними операторами? Один з найбільших операторів мобільного зв'язку в Україні Київстар запевняє, що так.

Інформація про те, що оператори можуть записувати або прослуховувати розмови абонентів – міф, – стверджують у прес-службі.

Якщо для розробки нових продуктів компанія потребує аналітичної інформації щодо переміщення абонентів, функції з відбору таких даних здійснюють інтелектуальні автоматичні IT-системи, дотримуючись принципів конфіденційності та анонімності процесів моніторингу.

Як захиститись?

Для того, аби не дозволяти сучасним технологіям збирати про вас всі дані, слід бути обережнішим, користуючись телефоном.

Зокрема експерт рекомендує:

– Ніколи не користуватися безкоштовними і неперевіреними сервісами. – Уважно вивчати сервіси, якими ви користуєтеся. Можна знайти інформацію про програму/сервіс на Reddit. Там часто обговорюють проблеми безпеки і «карму» компанії. Або ж можна переглянути новини пов'язані з ними.

– Можна використовувати пошукові системи, що не зберігають дані про вас, наприклад duckduckgo.

– У всіх нових месенджерах використовується end-to-end шифрування. В такому випадку тільки ви і адресат побачите повідомлення. В багатьох програмах воно за замовчуванням вимкнене та вимагає створення окремого чату. Наприклад секретний чат в Telegram.

– Якщо ви хочете якомога менше інформації про себе віддавати, слід замінити Google Chrome на Mozilla Firefox, і не логінитись в Google-сервісах.

– Уважно читайте до чого хоче отримати доступ черговий додаток, і думайте, навіщо воно йому. Деякі додатки можуть спробувати переконати вас, що це необхідно. Messenger Facebook попросить доступ до контактів, що б знайти ваших знайомих, яких ви ще не додали в друзі.

(вгору)

Додаток 28

7.11.2018

Они читают ваши сообщения: как найти безопасный мессенджер

Вы уверены, что ваша переписка в мессенджере не интересует киберпреступников? Как бы не так. Обычно люди думают, что хакеры охотятся за переписками президентов и за аккаунтами директоров корпораций. Но госструктуры и корпорации выстраивают сложные системы безопасности и часто используют для общения закрытые каналы. А вот «рядовые»

пользователи общаются в удобных и привычных мессенджерах – не особенно беспокоясь об их безопасности. Взломать их ничего не стоит, так что можно «щелкать» десятками в день (InternetUA).

Следствие такой беспечности – взломы, утечки конфиденциальных фото, распространение вирусов, мошенничество. Чтобы защититься от злоумышленников, нужно понимать, какие мессенджеры наиболее уязвимы – и дважды думать, прежде чем обсуждать там свои секреты или кликать по ссылке в сообщении. Но перед тем, как составить рейтинг и оценивать безопасность мессенджеров, стоит определить критерии.

Шифрование сообщений

Чтобы разобраться, как работает шифрование, представим двух пользователей. Когда один отправляет другому сообщение в мессенджере, оно сначала попадает на сервер, а оттуда пересылается на устройство http://internetua.com/oni–csitauat–vashi–soobsxeniya–kak–naiti–bezopasnyi–messendjer

Сообщение не просто проходит сквозь сервер, но и хранится на нем. Если хакеры взломают сервер, они смогут прочитать все сообщения, которые там есть. Еще один способ «поймать» чужое сообщение перехватить данные при отправке.

Чтобы защитить данные, компании-производители мессенджеров используют шифрование: даже если сообщение попадет в чужие руки, злоумышленник не сможет его прочесть без специального секретного ключа.

Как работает шифрование

Существуют разные подходы к шифрованию. Например, сквозное шифрование (End-to-End Encryption) – это механизм, при котором доступ к переписке имеют только отправитель и получатель. У обоих есть секретный ключ. Сквозное шифрование происходит по такому алгоритму:

– отправитель набирает сообщение на своем телефоне – и программа зашифровывает его секретным ключом;

– в зашифрованном виде сообщение попадает на сервер;

– с сервера сообщение пересылается на телефон получателя;

– программа на телефоне получателя использует секретный ключ и расшифровывает сообщение, то есть получатель видит уже обычный текст.

Ни отправителю, ни получателю не надо знать ключ. Его знает сама программа. Но и здесь есть сложность: если ключ шифрования один, то его могут перехватить. Чтобы защититься от такого сценария, используют ассиметричное шифрование. В этом случае используется два ключа: один публичный, который можно пересылать по незащищенному каналу, а второй – частный и не пересылается в исходном виде, хранится на устройстве. Частные ключи у отправителя и получателя разные, они создаются независимо.

Резервное копирование переписки

Бэкапы (копии) сообщений хранятся на облачных серверах в зашифрованном виде, но на том же сервере может храниться и ключ для расшифровки. Это небезопасно и напоминает ситуацию, когда пароль от

компьютера записывают на стикере и крепят к монитору, чтобы не забыть. Это как написать на банковской карточке ее PIN-код.

Представим, что пользователь уронил телефон в воду. В сервисном центре говорят: восстановлению не подлежит. А как мы помним, при более надежном ассиметричном шифровании частный ключ должен храниться в этом самом смартфоне. Человек покупает новый телефон, устанавливает на него мессенджер, вводит логин и пароль – и у него подгружается вся прошлая история переписки.

Такая ситуация доказывает, что на сервере хранились не только копии сообщений, но и копия ключа шифрования. Поэтому важно знать, на каких серверах мессенджер хранит историю переписки, надежна ли их защита.

Где хранят вашу переписку

Если бэкап хранится на сервере третьих лиц (например, Google), мессенджер снимает с себя ответственность за возможный взлом, перекладывая заботу о защите на другую компанию.

Но даже когда мессенджер использует собственные сервера для хранения переписки, все равно есть дополнительные риски. В этом случае многое зависит от лояльности руководства, скажем, к властям. Госструктуры вполне могут запросить доступ к переписке пользователей.

Например, в 2015 году, вскоре после атаки ИГИЛ в Париже, мессенджер Telegram обвинили в том, что этот канал связи используют для общения террористы. Тогда компания закрыла каналы террористов, но отказалась давать больше информации спецслужбам.

Разработчики заявили, что физически не смогли бы выдать ключи для расшифровки сообщений в каналах, так как ключи разбиваются на несколько частей, хранящихся на серверах по всему миру. Таким образом, чтобы дешифровать одно сообщение, силовикам нужно было бы получить разрешение на доступ у правительств нескольких стран. По крайней мере, такой была версия компании.

Есть мессенджеры, которые вообще не хранят историю переписки на сервере. В этом случае устройство (ваш телефон, например) является одновременно и клиентом, и сервером. Это самый безопасный способ, но мессенджеры «без истории» не пользуются популярностью. Одна из причин – мультиплатформенность мессенджеров с «облачной памятью»: вы можете войти в свой аккаунт одновременно на телефоне, планшете и компьютере.

Анонимность при регистрации и использовании

Еще один важный критерий – данные, которые используются при регистрации. Если аккаунт мессенджера привязан к номеру телефона, это дает злоумышленникам довольно простой путь для перехвата пароля. Перехват СМС осуществить проще, чем пытаться расшифровывать переписку.

Даже двухфазная аутентификация не защищает от риска, что злоумышленник удалит все данные из аккаунта, нанеся этим ущерб.

Обзор защищенности мессенджеров

Теперь оценим самые популярные мессенджеры среди украинцев по выбранным критериям. Все данные взяты из открытых источников: статей авторитетных СМИ, официальной документации самих мессенджеров.

Viber

Viber – самый популярный мессенджер в Украине, программой пользуется более 20 млн украинцев.

Сквозное шифрование: да – основано на протоколе Signal и включено по умолчанию, даже в версии для компьютера.

Сообщения хранятся: на серверах Apple iCloud и Google Drive (как мы помним, это не очень хорошо).

Секретные чаты: да.

Возможность анонимной регистрации и работы: нет.

Telegram

Сквозное шифрование: да, но по умолчанию чаты не шифруются (доступно только для секретных чатов).

Сообщения хранятся: на собственных серверах, расположенных в разных странах (по заявлению представителей компании, ни один из серверов Telegram не находится на территории России).

Секретные чаты: да.

Возможность анонимной регистрации и работы: нет.

Facebook Messenger

Сквозное шифрование: да, для секретных чатов.

Сообщения хранятся: в собственных дата-центрах.

Секретные чаты: да, но не по умолчанию. Начать секретный чат можно при помощи кнопки Secret при старте диалога.

Возможность анонимной регистрации и работы: нет.

WhatsApp

Сквозное шифрование: да.

Сообщения хранятся: на сторонних серверах iCloud, Google.

Секретные чаты: нет.

Возможность анонимной регистрации и работы: нет.

Пожалуй, безопаснее всего выбирать более защищенные мессенджеры – вроде Signal, Threema или Confide. Но эти приложения не очень-то популярны среди украинских пользователей, поэтому пользователи рискуют остаться в гордом одиночестве и тишине.

Но есть несколько способов сделать общение в «традиционных» мессенджерах более безопасным:

– Если есть возможность, давайте малознакомым людям не номер телефона, а никнейм.

– Заведите аккаунт в мессенджере на отдельный телефонный номер, который не привязан к онлайн-банкингу и другим важным сервисам.

– Настройте пароль для разблокировки смартфона и не оставляйте телефон без присмотра в общественном месте. Некоторые телефоны позволяют установить отдельный пароль на доступ к приложению.

В целом, нужно помнить, что ни один мессенджер не может обеспечить 100 % гарантии безопасности. Поэтому конфиденциальную информацию лучше передавать тет-а-тет. Кому-то такой подход покажется паранойей, но ведь беспечность и безопасность – несовместимы.

(вгору)

Додаток 29

7.11.2018

Новая версия Opera для Android позволяет блокировать назойливые уведомления

Недавнее вступление в силу Общего регламента защиты данных (GDPR) было направлено на повышение контроля пользователей над своей конфиденциальностью в сети (ITnews).

Однако, побочным эффектом этой инициативы стало то, что при посещении сайты стали повсеместно и зачастую довольно назойливо запрашивать у пользователей согласия со своими политиками конфиденциальности. Opera сегодня стала первым браузером, позволяющим пользователям отключать такие уведомления.

С 7 ноября пользователи могут улучшить свой опыт работы в сети, скачав последнюю версию браузера Opera на свой смартфон или планшет Android. В новой версии браузера Opera появился встроенный блокировщик окон об использовании cookie-файлов, который при активации блокирует все такие окна на том или ином сайте. Ежедневный браузинг пользователей с этой функцией станет проще и удобнее, позволяя им фокусироваться только на интересующем их контенте.

«У нас в Opera есть давняя традиция быть первыми, когда речь заходит о внедрении новых функций, улучшающих опыт работы людей в сети. Сегодня мы приглашаем пользователей попробовать наш блокировщик cookie-диалогов и тем самым избавиться от этого довольно серьезного раздражителя в процессе браузинга», – отметил Питер Вальман, старший вице-президент разработки браузера Opera.

Блокировщик cookie-диалогов может быть активирован в настройках браузера в разделе «Блокировка рекламы». При этом данная функция не запрещает сайтам использовать cookie-файлы. Для этого в Opera есть отдельная функция, позволяющая пользователям выбирать, принимать все или никакие cookie-файлы или же блокировать сторонние cookie-файлы.

Для блокировки cookie-диалогов Opera использует комбинацию правил CSS и эвристических алгоритмов JavaScript. Блокировщик был уже протестирован на 15 тысячах сайтов, и это количество будет увеличиваться, так как функция находится в постоянной разработке. Пользователи Opera могут также помочь приоритизировать, какие сайты необходимо раньше всего включить в этот список, отправив команде браузера уведомление с помощью соответствующей функции, встроенной в бета-версию браузера Opera.

В новой версии Opera для Android появились также клавиши быстрого доступа для домашнего экрана. Пользователи с версией Android 7.1 и выше могут теперь кликнуть на иконку лого О и увидеть клавиши быстрого доступа, с помощью которых можно начать новый поиск, отсканировать QR-код или открыть новую приватную вкладку. Вдобавок, пользователи могут также воспользоваться клавишей быстрого доступа для того или иного сайта на домашнем экране устройста, нажав и удерживая кнопку новой вкладки «+».

Кроме того, Opera также включила новую настройку размера текста, которая доступна в основном меню и позволяет менять размер текста на сайтах. Если веб-сайт не оптимизирован для мобильного браузинга, то эта функция позволяет сделать просмотр таких сайтов более комфортным.

Opera предоставляет больше контроля

В Opera мы верим, что у пользователей должно быть больше контроля над всем процессом браузинга. Вот почему мы включили такие продвинутые функции, как:

* Управление cookie с возможностью заблокировать все сторонние cookie-файлы.

* Удаление приватной информации, в том числе истории посещений, cookie, паролей и данных для автозаполнения форм.

* Приватный режим. Использование этого режима позволяет не сохранять какой-либо истории браузинга.

* Блокирование всплывающих окон.

* Экономия трафика. Обеспечивает более быстрый браузинг в сетях с медленным соединением и экономит до 60 % данных.

* Встроенный блокировщик рекламы.

* Принудительное масштабирование. Некоторые сайты не разрешают пользователям менять размер верстки сайта. Данная функция позволяет обойти это ограничение и менять масштаб любого сайта.

* Перенос текста: уникальная функция, подгоняющая текст под размер экрана телефона.

* Контроль разрешений для сайтов. Получите полный контроль над элементами вашего устройства, к которым могут получить доступ некоторые сайты, в том числе местоположение, камера или микрофон.

* Идентификация как мобильного или десктопного браузера. Зашли на мобильную версию сайта без всех десктопных функций? Переключите режим для смены версии.

Доступен для скачивания

Opera доступна для скачивания в Play Маркете. Функция блокировки cookie-диалогов сегодня эксклюзивно доступна в браузере Opera для Android, но ее планируется реализовать вскоре и в других продуктах Opera.

(вгору)

Додаток 30

8.11.2018

Як смартфон стежить за вами

Маленькі пристрої, які кожен носить у кишені, не лише постачають своїм власникам інформацію, але й збирають її (InternetUA).

В кінці 2017 року стало відомо, що Google стежить за користувачами Android. З початку 2017 року компанія збирала дані про місцезнаходження Android-пристроїв, навіть якщо на гаджетах були вимкнені сервіси визначення геолокації.

Навіть скинуті до заводських налаштувань пристрої відправляли геолокацію в Google.

В результаті компанія мала доступ до даних про місцезнаходження окремих осіб і їхнє переміщення, що, ймовірно, не виправдовувало очікування споживачів щодо конфіденційності.

Тоді Google визнав, що збирає такі дані протягом майже року, але пообіцяв прибрати цю функцію.

Однак, як виявилось, це не єдиний підводний камінь, який чекав на користувачів.

Google–пошук

Видання Quartz провело дослідження трьох різних телефонів на базі операційної системи Android, перевіривши, яка саме особиста інформація користувачів потрапляє на сервери Google.

Незалежно від того, чи був телефон підключений до мережі, він передав перелік типів переміщень (наприклад, відсоткове співвідношення ходьби, їзди на велосипеді та в автобусі за день) та дані вбудованого барометру, які допомагають прогнозувати погоду та більш точно визначати місце знаходження.

При підключені до мережі Wi-Fi, смартфон повідомляв MAC-адресу, яка є унікальним ідентифікатором точки доступу Wi-Fi, до якої підключений користувач, силу сигналу кожної з точок Wi-Fi поблизу, а також ідентифікатор і потужність сигналу Bluetooth.

Крім того, на сервери Google відправлявся рівень заряду акумулятора телефону і те, чи телефон заряджається. Та, що важливо, координати GPS телефону та точність цих координат.

Як зазначили у виданні, це справді тривожні дзвіночки, враховуючи, що більшість людей навіть не знає про те, що вони погоджуються поділитися своєю історією місцезнаходжень з компанією.

Також виявилось, що тільки-но ви надаєте будь-якому з додатків Google на вашому телефоні доступ до історії місцезнаходжень, наприклад, картам, з якими складно працювати без геолокації, решта додатків Google також отримує ці дані.

В розділі політики конфіденційності Google зазначено, що компанія буде збирати інформацію про місцезнаходження пристроїв, що використовують її послуги, проте не зазначено, як саме.

В Google стверджують, що роблять це для забезпечення кращих результатів пошуку та рекомендацій для користувачів.

«Наприклад, ви можете отримувати прогнози заторів, переглядати фотографії, згруповані за місцем, отримувати рекомендації на основі відвіданих місць і навіть знайти загублений телефон», – коментують виданню ситуацію в Google.

В компанії також зазначають, що це особистий вибір кожного, службу локації можна вимкнути. Однак, якщо це зробити, доступ до деяких додатків може бути закритий.

Ще одна небезпечна річ, яку може робити смартфон і про яку можна не здогадатись – це функція «Ваші місця», які Google формує самостійно.

У всіх смартфонах є GPS-модуль, за допомогою якого пристрій визначає місцезнаходження та прокладає потрібний маршрут. Телефон запам'ятовує всі місця, які відвідуються і коли. Їх можна переглянути в Google Maps.

А якщо не Android

Якщо ви власник iPhone – це, звичайно, привід радіти, але не такий великий, як здавалося б. Незважаючи на те, що iPhone вважається більш захищеним, тут також є свої причини для засмучення.

По-перше, Google збирає інформацію за допомогою усіх своїх сервісів. Тобто навіть якщо смартфон на iOS, а не на Android, проте власник користується пошуковою системою Google, вся інформація зберігається.

Якщо до всього цього користувач ще використовує пошту Gmail, інформація на усіх пристроях, з яких він залогінився у пошту, синхронізуються. Тобто, те, що ви шукали з телефона може раптом з'явитися у вигляді контекстної реклами на робочому комп'ютері.

Наприклад, був випадок з Михайлом Добкіним, коли він звинуватив Українську правду в неперебірливості рекламою, хоча реклама було контекстною і до неї цілком могла призвести саме техніка «крос-пристрою».

По–друге, смартфони Apple також були помічені у шпигунстві. Останнього разу інженер компанії Google виявив проблему з налаштуваннями приватності в iOS, яка дозволяла програмам на iPhone вести приховану зйомку.

Для цього додатку досить було отримати від користувача дозвіл на доступ до камери, після чого він міг в будь-який час робити фото і записувати відео з фронтальної та основної камер.

Під ковпаком

Величезна кількість інформації може бути зібрана зі смартфонів незалежно від їх виробника, як під час активного використання, так і під час роботи в фоновому режимі.

Ця інформація може включати місце розташування користувача, історію пошуку в інтернеті, активність у соціальних мережах, рівень доходів та біометричні дані.

Якщо давати доступ до цієї інформації якомусь додатку, треба пам'ятати, що він може передавати її, кому заманеться. Внаслідок цього сторонні компанії

можуть відслідковувати, де ви знаходитесь, як швидко ви рухаєтеся і що взагалі робите.

Дуже мало програм публікує свою політику щодо конфіденційності користувачів, але навіть якщо вони це роблять, зазвичай це довгі юридичні документи, які більшість людей не читає і не розуміє.

Ніхто не пише прямо: «Ви можете дати нам доступ до своєї телефонної книги, але, можливо, вам та вашим друзям прийде кілька смс від таксі», як це нещодавно було з додатком GetContact.

За даними дослідження, сім з десяти мобільних додатків відправляють зібрану інформацію третім особам.

Інтернет-ідентифікація користувачів не захищається законодавством. Дослідження показує, що дані проходять через національні кордони і часто потрапляють до країн із «недружніми» законами про конфіденційність. Такими як США, Великобританія, Франція, Сінгапур, Китай та Південна Корея – шість країн, де впроваджені технології масового спостереження.

Відстежуючи весь потік даних, смартфони формують детальний профіль свого користувача. Вони можуть розповісти про інтереси користувача, його вподобання, політичні чи релігійні погляди, сексуальну орієнтацію та інше.

При цьому дані з різних програм доповнюють один одного. Таким чином смартфон збирає на користувачів чималі портфоліо, які можуть продаватися між компаніями без попередження, а тим більше згоди.

Найбільш очевидною причиною для компаній, що збирають інформацію про фізичних осіб, є отримання прибутку, надання цільової реклами та персоналізованих послуг.

Це може вилитись у те, що наступного разу реклама Google запропонує вам потрібні курси, про які ви вже давно думали, що насправді зручно. Або ж, навпаки, приховає від вас оголошення про оренду житла, якщо ви належите до певної етнічної групи, яка не імпонує орендодавцю, або оголошення про роботу, якщо ви не відповідаєте віковим вимогам роботодавця.

Крім того, дані соціальних мереж, незважаючи на їх сумнівну достовірність, також можуть використовуватися для розрахунку кредитоспроможності.

Неможливо передбачити та виявити повний спектр способів, якими смартфон може збирати та використовувати вашу інформацію. Наведені вище факти – це лише невелика частка того, що вже стало відомо.

Єдине можна сказати напевно: смартфони є своєрідними пристроями спостереження 21 сторіччя, і всі, хто їх використовує, в певній мірі ризикують.

(вгору)

Додаток 31

12.11.2018

Владимир Кондрашов

Полиция поймала украинца, который 8 лет продавал «орудия взлома»

Гражданин Украины около восьми лет через собственный интернет-магазин и на специализированных форумах в даркнете продавал так называемые «дедики» (dedicated server – удаленный сервер с мощной аппаратной конфигурацией, используемый злоумышленниками для брута, спама, флуда, DDoS-атак и т. д.). Найти злоумышленника удалось только сейчас (InternetUA).

Об этом пишет InternetUA со ссылкой на определение Винницкого городского суда Винницкой области.

Как стало известно из определения суда, путем проведения оперативно-розыскных мероприятий полицейские установили личность жителя Винницы, который получает доступ с правами администратора к серверному оборудованию, без разрешения его владельцев, путем произвольного сканирования сети Интернет и дальнейшего подбора логина и пароля.

– В ходе осуществления проверки полученной информации установлено, что последний базируется на специализированных интернет-форумах, где размещает объявления о продаже «dedicated server», а также имеет собственный Интернет магазин (www.bestrdp.deer.is), – говорится в материалах дела. – Также установлено, что после несанкционированного доступа к серверному оборудованию житель Винницы, используя в Интернет сети никнейм «Akvelon», размещает объявления о продаже программного обеспечения для удаленной аутентификации третьими лицами. Последний осуществляет свою деятельность на протяжении длительного времени (примерно с 2011 года).

Также мужчину подозревают в продаже «dedicated server», которые размещены на серверном оборудовании как на территории Украины, так и в зарубежном сегменте.

Одно из объявлений пользователя Akvelon, которое до сих пор доступно в сети. Мужчина зарегистрировался на форуме еще в 2006-м году.

Также полицейским удалось установить электронный кошелек «Webmoney», который «Akvelon» использовал для принятия оплаты при покупке dedicated server. Персональный аттестат Webmoney был выдан персонализатором в Виннице.

На данный момент следствие продолжается. Решением суда полицейские получили доступ к вещам и документам провайдера, услугами которого пользовался мужчина: следствие получит копию договора о предоставлении услуг доступа к глобальной сети Интернет по адресу и сведения о имеющемся сетевом интернет-трафике в период с 01.08.2018 года по настоящее время.

(вгору)

Додаток 32

12.11.2018

Злоумышленники атакуют сайты на WordPress через популярный плагин

Киберпреступники активно эксплуатируют уязвимость в популярном плагине WP GDPR Compliance для установки бэкдоров и перехвата управления сайтами на WordPress. Данный плагин помогает владельцам ресурсов обеспечить соответствие требованиям Общего регламента по защите данных (GDPR), число его установок превышает 100 тыс (InternetUA).

Атаки на сайты начались примерно три недели назад. Как показало расследование, на всех пострадавших ресурсах был установлен плагин WP GDPR Compliance. Команда WordPress удалила плагин из каталога в связи с наличием ряда уязвимостей в его коде. Плагин был восстановлен в каталоге после выпуска исправленной версии 1.4.3.

Несмотря на выпуск новой версии плагина многие владельцы сайтов еще не установили обновление, чем и пользуются киберпреступники, продолжая атаковать ресурсы, использующие уязвимые редакции WP GDPR Compliance (версия 1.4.2 и ниже).

По словам специалистов компании Defiant, злоумышленники применяют атаки двух типов. В первом случае они используют уязвимость в плагине для модификации настроек и создания новой учетной записи администратора и устанавливают на скомпрометированном сайте бэкдор (файл wp-cache.php), позволяющий загружать дополнительные вредоносные модули.

Во втором случае атакующие добавляют новую задачу в WP-Cron – встроенный планировщик задач WordPress. Данный процесс загружает и устанавливает плагин 2MB Autocode, который злоумышленники в дальнейшем используют для внедрения бэкдора на сайт. Файл обладает тем же именем (wp-cache.php), но отличается от указанного выше.

В настоящее время атакующие просто компрометируют сайты и не используют бэкдоры для каких-либо вредоносных действий. С какой целью проводятся атаки, пока неясно. Как полагают исследователи, атакующие могут готовить инфраструктуру для будущих кампаний или «копят» ресурсы для дальнейшей продажи доступа к ним другим киберпреступным группировкам.

(вгору)

Додаток 33

12.11.2018

Почему не стоит пользоваться сторонними клиентами Telegram

Альтернативные клиенты Telegram могут быть небезопасны, подвергая риску переписку своих пользователей, сообщают авторы канала «Телеграм Технарь». Несмотря на строгие правила использования API, не позволяющие отключать шифрование сообщений, разработчики сторонних клиентов теоретически могут иметь к ним доступ, нарушая таким образом право пользователей на тайну переписки, за соблюдение которого так ратует руководство Telegram и сам Павел Дуров (InternetUA).

Telegram, давно переросший статус просто удобного мессенджера в оплот безопасного общения, всячески способствует созданию сторонних клиентов,

старательно популяризуя свой API. По словам представителей сервиса, основным преимуществом клиентов от независимых разработчиков является более широкий набор функций. В частности, они без проблем могут дополнять исходный мессенджер новыми возможностями, но физически не могут приуменьшить те, что доступны по умолчанию.

Можно ли перехватить сообщения в Telegram

Впрочем, уточняют авторы «Телеграм Технарь», разработчики могут только пообещать не перехватывать сообщения, которые отправляются через их приложения, но при должной подкованности способны нарушить данное обещание, не говоря о массе других изъянов. Хуже всего, что на деле они практически не несут ответственности за утечку, а самая серьезная санкция, которая может за этим последовать, – прекращение отношений с Telegram и удаление скомпрометированного приложения из App Store.

В качестве примера «Телеграм Технарь» приводит сторонний клиент Teleplus, который до недавнего времени был доступен в фирменном каталоге приложений Apple и пользовался сравнительной популярностью из-за способности разделять группы, каналы и личную переписку по вкладкам. Правда, недавно Teleplus исчез из App Store, поскольку нарушал политику Telegram. Мало того что клиент не отличался высокой стабильностью, так еще и вставлял рекламу везде, где только можно.

(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.