СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.03–10.04)

2018 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.03–10.04)
№ 7

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

29.03.2018

Facebook разрешит пользователям удалять собранную о них информацию

Социальная сеть Facebook опубликовала информацию о новых функциях, с помощью которых можно будет сделать свой аккаунт безопаснее. Обновления появились после того, как соцсеть обвинили в незаконной передаче персональных данных Cambridge Analytica. Запись опубликована в блоге компании, передает «Радио Свобода» (InternetUA).

Теперь пользователи смогут удалить информацию о друзьях, истории поиска, лайках и комментариях. Изменения коснулись меню настройки приватности, которое стало более доступным и понятным. Также пользователям будет предоставлено больше возможностей для защиты своего аккаунта от взлома и кражи, например двухфакторная аутентификация.

***

1.04.2018

Facebook требовал от сотрудников увеличения аудитории любой ценой

Один из наиболее влиятельных менеджеров Facebook Эндрю Бозворт, известный как Боз, рекомендовал своим сотрудникам использовать любые методы, если они помогают увеличить аудиторию соцсети, следует из его письма подчиненным, опубликованного Buzzfeed.

Докладніше

***

1.04.2018

В Twitter появилась возможность публиковать отдельные моменты видеотрансляций

Twitter представила функцию Timestamps, которая позволяет поделиться ключевым моментом прямой трансляции. Зрителям больше не нужно проматывать до той части видео, которую вы хотите обсудить (InternetUA).

Раньше в Twitter можно было опубликовать только полную запись трансляции. Если вы хотели подчеркнуть какой-то конкретный отрезок видео, то вам приходилось писать, до какого момента зрителям нужно промотать ролик. Особенно мучительно это тогда, когда человек публикует длинную запись.

Функция Timestamps значительно упрощает процесс. Теперь, когда вы решите поделиться трансляцией или её записью, то сможете промотать до того отрезка, который хотите показать своим подписчикам. Затем останется добавить текстовый комментарий и опубликовать твит.

Зрители, включив ролик, начнут его просмотр с того момента, который вы указали при публикации. Если трансляция всё ещё идёт, то пользователь сможет нажать на иконку Live и просмотреть нужный отрезок.

Нововведение отлично сочетается с трансляциями в Twitter спортивных мероприятий. Также Timestamps может быть полезна тем, кто хочет поделиться любимой песней с концерта, а репортёры смогут подчёркивать самое важное на пресс-конференциях. Функция в ближайшее время станет доступна всем пользователям веб-версии Twitter и приложений для iOS и Android, а также Periscope.

***

3.04.2018

Пользователи Skype Interviews могут использовать общую электронную доску

Сервис онлайн-собеседований Skype Interviews уже имеет ряд уникальных функций – например, редактор кода, работающий в реальном времени. Он позволяет оценивать умение кандидатов писать код, не прибегая к каким-либо сторонним приложениям. Есть еще есть планировщик для рекрутеров и другие полезные функции (Компьютерное Обозрение).

Недавно в продукт добавлена также электронная доска (whiteboard), с помощью которой можно демонстрировать диаграммы, визуализировать задачи и представлять идеи в графическом виде.

Доска отражает движение курсоров обоих участников, благодаря чему гораздо проще следить за направлением мыслей собеседника.

Электронная доска предлагает широкий набор инструментов, с помощью которых можно делать наброски сложных планов, показывать порядок действий и сохранять изображение доски для дальнейшего использования. В конце интервью можно сохранить копию доски в формате SVG.

Сейчас доступна предварительная версия Skype Interviews.

***

3.04.2018

Олег Дмитренко

«Вконтакте» вперше не потрапив в ТОП-10 сайтів за відвіданістю в Україні

Згідно з інформацією щомісячного дослідження Kantar TNS CMeter, «ВКонтакте» вперше випав з ТОП-10 сайтів за відвідуваністю серед українців (Watcher).

Зменшилось охоплення і у лідера українського ринку електронної комерції – Rozetka. При цьому китайський Aliexpress.com в березні додав 2 % охоплення.

Тривала зима не давала спокою українцям, які стали частіше перевіряти погоду і підняли охоплення Sinoptik.ua і Gismeteo.ua на майже 3 % і 4 % відповідно.

***

4.04.2018

В Snapchat запустили групповые видеозвонки

Разработчики популярного приложения Snapchat выпустили обновление, добавляющее интересные новые возможности. Во-первых, речь идет о групповых видеозвонках (InternetUA).

Пользователь может запустить видеоконференцию с 16 друзьями одновременно. Для этого достаточно нажать на пиктограммку видеокамеры в групповом чате. Участники чата получат оповещения с приглашением присоединиться к видкозвонку.

Ещё одно новшество – Mentions (упоминания). Mentions позволяют ставить теги-ссылки на друзей в своих историях, почти как в Twitter или Facebook. Если набрать @ИмяПользоввателя в вопросе, то нужный пользователь будет оповещен и приглашён в чат. Также такие упомянутые аккаунты можно легко просмотреть и добавить в друзья.

***

5.04.2018

Facebook сделала персонажей VR-соцсети Spaces более правдоподобными

Facebook добавила в VR-соцсеть Spaces новые возможности настройки персонажей. Раньше можно было изменять лишь небольшое количество параметров вроде цвета волос и формы глаз – тело нельзя было настраивать вообще. Теперь вариантов настройки аватаров – несколько сотен. Они станут доступны всем пользователям на этой неделе (InternetUA).

«Наша цель – позволить каждому показать в виртуальной реальности настоящего себя, и мы знали, что в этом плане можем достичь большего, – заявила компания. – Чтобы добиться полноценного социального опыта в виртуальной реальности, вам нужен привлекательный аватар, который представляет вас и помогает общаться с другими людьми в виртуальном пространстве. Это имеет огромное значение для достижения полноценного эффекта присутствия. Поэтому мы постоянно изучаем то, что помогает людям выражать себя, проводя время с друзьями в виртуальной реальности».

Spaces находится в стадии открытого бета-теста и доступна владельцам Oculus Rift и HTC Vive.

***

5.04.2018

В WhatsApp появились сразу несколько новых функций

Разработчики WhatsApp добавили в популярный мессенджер сразу несколько новых возможностей. Об этом пишет ресурс Digit.in (InternetUA).

Теперь пользователи приложения смогут просматривать последние обновления статуса прямо на экране виджетов, а также воспроизводить аудиосообщения вне окна чата. Таким образом, больше не нужно будет оставаться в программе, чтобы прослушать все звуковые послания.

Пока нововведения стали доступны только для владельцев устройств под управлением iOS 7.0 и выше. Пользователи Android смогут оценить новые функции в скором времени.

***

9.04.2018

Facebook повідомить, чи передали ваші дані Cambridge Analytica. І розповість, як захиститися

Починаючи з 19.00 за Києвом, Facebook повідомлятиме користувачам, чи є вони серед 87 мільйонів профілів, інформацію щодо яких передали компанії Cambridge Analytica.

Про це повідомлє CNBC (Espreso.tv).

Кожен власник профілю отримає одне з двох повідомлень щодо того, чи їхня приватна інформація постраждала.

У компанії також заявили, що людям покажуть, які додатки і яку інформацію з їхньою допомогою могли збирати. Так, ви зможете побачити посилання «захистити вашу інформацію» у верхній частині екрану новин.

Коли ви натисните на нього, то перейдете в розділ, де побачите, які програми та веб-сайти використовувалися для входу в Facebook, і видалити їх або відімкнути від свого облікового запису.

***

10.04.2018

Skype разрешит записывать видео звонков

В этом году Skype исполняется пятнадцать лет. За эти годы сервис успел сменить владельца, архитектуру, покорить все современные платформы и отказаться от поддержки некоторых из них. Не успел лишь обзавестись функцией записи видео бесед (InternetUA).

В какой-то мере команда Skype намерена исправить ситуацию лишь в этом году, предложив своим пользователям новый продукт – Skype for Content Creators. Предназначен он, как можно догадаться из названия, в первую очередь

создателям контента – всем этим блогерам, стримерам, авторам видеоуроков, журналистам и прочей творческой братии.

Впрочем, собственно Skype записывать видео по-прежнему не сможет: такая возможность будет официально предоставлена сторонним приложениям, поддерживающим технологию NewTek NDI. В их числе такие программы как Wirecast, Xsplit и Wmix, например. Записанный звонок можно будет легко импортировать в Adobe Premier Pro и Adobe Audition для дальнейшего редактирования.

Заметим, что запись видео-звонков в Skype при помощи сторонних инструментов была возможна и ранее, но официально не поддерживалась. То есть вместо прежних кустарно изготовленных костылей пользователи Skype получили новенькие сертифицированны.

***

10.04.2018
Майя Яровая
Топ-5 мессенджеров в Украине: больше 90 % пользуются Viber

Среди мессенджеров во всем мире лидирует WhatsApp, а на втором месте Facebook Messenger (по данным Similarweb). Но не в Украине. Безоговорочное лидерство принадлежит Viber, которым как минимум раз в месяц пользуется 94 % владельцев смартфонов (около 40 % всего населения Украины). Facebook Messenger занимает второе место с огромным отрывом, а WhatsApp – один из наименее распространенных мессенджеров (AIN.UA).

Рейтинг мессенджеров и социальных сетей составлен компанией Admixer на основании данных исследования TNS за февраль 2018 года (Android)

В среднем пользователь Viber проводит в приложении 30 минут в день. 45 % этого времени составляют звонки и видеозвонки. Один пользователь отправляет 20+ сообщений в день, а 35 % пользователей пользуются стикерами. Размер аудитории в Украине на сегодняшний день компания не раскрывает.

WhatsApp охватывает только 22 % пользователей смартфонов в месяц, и его в Украине уже опередил Telegram с охватом 28 %. Также в нашей стране все еще популярен Skype (30 %).

Среди соцсетей после запрета российских сайтов в Украине уверенно лидирует Facebook с охватом 65 %. Некогда лидирующая соцсеть «ВКонтакте» (39 %) сегодня уступила место Instagram (48 % охвата) и занимает третье место. Примечательно, что на четвертом – Google+ с 13 % охвата, а на пятом «Одноклассники». Столь низкую позицию второй российской соцсети объясняют тем, что аудитория «Одноклассников» преимущественно более зрелого возраста и в основном заходит с компьютера, в исследовании же учитывали именно приложения.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

2.04.2018
Михаил Сапитон
Opendatabot запустил уведомления о судебных делах через мессенджеры

Проект Opendatabot запустил возможность удаленно узнавать об открытии и обновлении статуса судебных дел. Для этого нужно найти в боте (доступен для Skype, Telegram, Facebook и Viber) свою компанию или ФЛП, выбрать опцию «Поиск в судебных делах» и подписаться.

Докладніше

***

31.03.2018
Флешмоб перевір пожежний вихід в Києві триває: активісти взялися за лікарні

У Києві триває флешмоб: #перевірпожежнийвихід. На цей раз проблеми з протипожежною безпекою помітили в одній з київських лікарень. Про це в Facebook повідомив Владислав Бовсуновський (УНН).

«З цікавості зайшов в стаціонар і перевірив входи/виходи, включаючи аварійні. Усі закриті. Пішов розбиратися: виявилося, закриває старша медсестра щоб діти не виходили. На моє запитання про те, що буде в разі пожежі, вона лише розвела руками. До речі, пошук цієї загадкової жінки з ключами тривав хвилин 20», – написав чоловік, після відвідин однієї з київських лікарень.

Як повідомляв УНН, після пожежі в ТЦ «Зимова вишня» в російському Кемерово українці в соціальних мережах запустили флешмоб: #проверьпожарнийвиход.

***

9.04.2018
Флешмоб: жители Киева назвали самые опасные ТРЦ

Киевляне в социальных сетях объявили флешмоб #проверьторговыйцентр на предмет пожарной безопасности и начали выкладывать в Facebook свои наблюдения, сопровождая их фото.

Докладніше

***

6.04.2018

#РозкажиЯк: у мережі набирає обертів флешмоб про успішні приклади громадської активності

Під хештегом #РозкажиЯк активісти з різних міст України у соцмережах поширюють історії про те, як своїми діями змінюють громаду та спонукають громадян брати відповідальність за своє оточення.

Докладніше

***

5.04.2018

У мережі набирає обертів флешмоб у підтримку Уляни Супрун

Владика Ірина

На просторах Інтернету розпочався флешмоб #япідтримуюсупрун. Таким чином, деякі інтернет-користувачі засуджують можливе звільнення Уляни Супрун з посади виконувача обов'язків міністра охорони здоров'я.

Докладніше

***

28.03.2018

Жители Запорожья и области присоединятся ко всемирному флешмобу

Первого апреля в Украине стартует акция «30 дней на велосипеде» в рамках Всемирного флешмоба «30 days of biking» (vmeste).

По условиям акции каждый из участников должен на протяжении месяца ежедневно ездить на велосипеде и не пользоваться общественным транспортом и автомобилем. Затем каждый день участник флешмоба должен выкладывать в соцсети фотографии с хештегами #30daysofbiking или #30daysofbikingUA.

Для участия в акции нужно зарегистрироваться на официальном сайте: 30 days of biking.

Целью «велосипедного апреля» является популяризация активного образа жизни. В Украине данная акция пройдет уже в третий раз.

Велоакцию поддержат масштабными велопробегами жители Мелитополя, Бердянска и Запорожья.

***

6.04.2018

«Співати – не країною керувати». Як у соцмережах відреагували на заяву Вакарчука про бідне політичне меню

Христина Біляковська

У Києво-Могилянській академії відбулася відкрита зустріч з українським музикантом, лідером гурту «Океан Ельзи» Святославом Вакарчуком. У нього запитали про президентські амбіції. Відео відповіді Вакарчука опублікувала у Facebook Віола Денис, яка була на зустрічі. Вакарчук заявив, що українці справді хочуть бачити нові обличчя в політиці. «Якщо ви подивитеся на рейтинги, ви побачите цікаві цифри – за різними опитуваннями, від 50 % до 60 % населення України взагалі не може вибрати жодного політика або політичну силу з політичного меню «ресторану», яке нам пропонують. Це безпрецедентна історія, коли абсолютна більшість населення України не хоче вибирати з тих політиків, які є... Це дуже загрозлива ситуація. Такі ситуації бувають або перед великими позитивними змінами, або перед великими потрясіннями», – зазначив музикант. Ці його слова багато хто потрактував як натяк на майбутню участь у президентських виборах. Чи стане Вакарчук саме тим «новим обличчям» у політичному меню, за яке ми захочемо голосувати? «Молодець! Україні потрібні нові обличчя», – пише Валентина Маруча. Інші підійшли до питання з гумором: «Нам вже достатньо мера-боксера!», – обурюється Наталія Байда. Думки багатьох розділилися. А хтось вважає, що Вакарчук і президентство – поняття взагалі не сумісні (Експрес).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

28.03.2018
Facebook потерял $80 млрд: компании меньше доверяют

Акции социальной сети Facebook упали на 18 %, а рыночная капитализация компании сократилась на $80 млрд (U-News).

Трудности начались 16 марта. Тогда компания Facebook заявила, что приостанавливает анализ данных компании Cambridge Analytica, которая собрала личные данные более 50 млн пользователей соцсети.

Инвесторы обеспокоены тем, что Facebook, а также такие компании как Google и Twitter, могут столкнуться с более жесткими правилами во всем мире из-за споров вокруг Cambridge Analytica. Также есть опасения, что пользователи могут перестать пользоваться социальными сетями из-за проблем с конфиденциальностью. Если это произойдет, рекламодатели также откажутся от сотрудничества с Facebook.

По этой причине несколько аналитиков Wall Street снизили целевые цены и оценки прибыли для Facebook в течение последних полутора недель. Доверие к Facebook и других технологических компаний потеряно, считают аналитики.

***

3.04.2018
YouTube добавил формат коротких рекламных роликов

Теперь бренды могут покупать рекламу TrueView и оптимизировать ее для охвата. Это значит, что рекламодатели смогут создавать короткие ролики в шесть секунд (и до 30 секунд), которые пользователи могут пропустить через 5 секунд. Эти ролики будут демонстрироваться до или во время видео. Формат TrueView по охвату предполагает оплату за каждую тысячу просмотров не менее пяти секунд либо в случае взаимодействия пользователя с рекламой. За формат TrueView in-stream рекламодатели платили, когда зрители смотрели хотя бы 30 секунд ролика или до конца видео, или когда предпринимали действия, кликая на элементы креатива (Marketing Media Review).

***

9.04.2018

Соцсеть исправляется: как Facebook защитит данные пользователей

Из-за скандала, разгоревшегося вокруг политики конфиденциальности Facebook, руководство компании заявило о закрытии функции для создания таргетированной рекламы под названием «Партнерские категории».

Докладніше

***

10.04.2018

Стив Возняк высказался против политики Facebook и уходит из соцсети

Сооснователь Apple Стив Возняк раскритиковал Facebook и заявил, что покидает социальную сеть, «принесшую больше негатива, чем позитива». Причиной такого поступка стал сбор массивного объема данных о своих пользователях (InternetUA).

– Пользователи передают в Facebook каждую деталь своей жизни, и Facebook делает огромные деньги на рекламе. Она базируется на пользовательских данных, но юзеры ничего не получают взамен, – заявил Возняк.

Также изобретатель отметил, что лучше бы заплатил Facebook для сохранения приватности своей информации. В качестве положительного примера о защите данных пользователей Возняк назвал Apple: мол, корпорация зарабатывает на продукции, но в случае с Facebook сами люди и есть продукт.

Недавно и сам глава Apple выступил с критикой Facebook. По его словам, корпорация изучает каждое приложение сторонних разработчиков и проверяет, чтобы эти программы отвечали стандартам Apple касательно приватности.

Ранее стало известно об утечке данных 87 миллионов пользователей Facebook.

***

10.04.2018
Инвесторы требуют отставки Цукерберга с поста главы Facebook

Лишь вопросом времени было появление призывов о смещении Марка Цукерберга с поста главы Facebook в связи со скандалом о приватности, развернувшимся вокруг социальной сети. «Он не понимает, насколько большой мировой компанией руководит. У него сейчас две должности – директора и председателя правления Facebook. Пришло время отказаться от одного (или обоих) титулов», – заявил CEO Open Mic Майкл Коннор (InternetUA).

Он предлагает Цукербергу уйти в отставку по собственному желанию. Либо ожидать увольнения. Примечательно, что у Open Mic нет акций Facebook. Однако компания работала с инвесторами Facebook в части координации их запросов к компании.

Аналогичные предложения по смещению Цукерберга поступали от представителя муниципального пенсионного фонда Нью-Йорка, который уже является прямым инвестором Facebook.

Цукерберг в свою очередь в интервью The Atlantic заявил, что уходить не собирается, потому что уверен, «что может справиться с образовавшимися проблемами». Сам он точно не уйдет, так как владеет 60 % голосующих акций в компании.

Тем временем Марк дал показания комитету палаты представителей США по энергетике и торговле, где извинился за фейковые новости, иностранное вмешательство в выборы и утечку информации о пользователях.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

31.03.2018
Чудовища в Сети: как защититься от троллей?
Валентина Развилова

Среди интернет-комментаторов есть совершенно особенная порода людей, единственная цель которых – вывести из себя собеседника. Их называют троллями. Зачем они так себя ведут и как с ними общаться?

Докладніше

***

29.03.2018

Ученые: Соцсети негативно влияют на жизнь подростков

Британские ученые заявили, что социальные сети оказывают крайне негативное влияние. По их мнению, длительное время, проведенное в интернете, катастрофически снижает вероятность дальнейшего благоустройства подростков, в особенности девочек (Аспекты).

В ходе проведения исследования эксперты установили гендерные различия, которые касаются времени использования социальных сетей. Исследователи уверены, что особо отрицательное воздействие проявляется на девушках-подростках и приводит к понижению шансов на благополучие в последующей жизни.

Особое внимание ученые обратили на ответы опрашиваемых в возрасте от 10 до 15 лет. После этого серию полученных данных сравнили с результатами, которые описывают социально-эмоциональные трудности, с которыми сталкиваются подростки, и уровень их счастья. Оказалось, что 14-летние девочки намного чаще использовали смартфоны для входа в социальные сети, чем мальчики того же возраста.

***

3.04.2018

«Вдыхание кондомов»: среди подростков распространяется опасный флешмоб

Подростки резко вдыхают презерватив через одну из ноздрей. Позже его вытягивают пальцами изо рта. Особым мастерством считается исполнение данного процесса без помощи рук. Видеоролики, на которых подростки вдыхают презервативы через нос, набирают популярности в сети. На это явление обратил внимание американский телеканал 12news. Новый челлендж назвали «вдыханием кондомов» (Condom snorting challenge). Сюжет вирусных видео состоит в резком втягивании контрацептива через одну из ноздрей. Впервые видео подобного содержания появились пять лет назад, однако только сейчас этот трюк стал сюжетом вирусных роликов. Эксперты отмечают, что каждый новый челлендж, распространяемый среди подростков, опаснее предыдущего, потому что тинейджеры готовы на многое ради популярности в сети (ukrnews24.net).

***

3.04.2018

Не перетворюйтеся на пластик: черкащанка розповіла як реагувати на хейтерство та тролінг у соцмережах

Що робити з «тролями» та «хейтерами», чи видаляти незручні запитання і коментарі та чи варто розділяти «себе-людину» та «себе-професіонала», розповідає Олена Литвинова, черкащанка, яка заробляє блогерством на життя.

Докладніше

***

6.04.2018
Проводячи час у соцмережі, можна позбутися стресу

Вчені з Університету Квінсленда дійшли висновку, що утримання від відвідування соцмереж призводить до зниження рівня гормону кортизолу, який відповідає за стан стресу (Наша мама).

Дослідники спостерігали за 138 активними користувачами соціальної мережі Facebook. Всім їм було запропоновано відмовитися від відвідування сайту на 5 днів. Учасники експерименту пройшли обстеження до і після своїх вимушених «канікул» у соцмережах, зокрема, вони здавали слину для вимірювання рівня кортизолу.

Виявилося, що навіть 5-денна відмова від відвідування соцмереж призводить до значного зниження рівня кортизолу в організмі, тобто люди відчувають менший фізіологічний стрес. Однак при цьому випробовувані повідомили про зниження почуття задоволеності життям. Вони зізналися, що відчували себе нещасними і з нетерпінням чекали відновлення спілкування на сторінках Facebook. Їм здавалося, що вони відрізані від своїх друзів.

Вчені рекомендують робити подібні перерви на кілька днів, щоб давати організму відпочинок від інтенсивного віртуального спілкування. Після цього можна продовжувати спілкуватися, оскільки соціальні мережі міцно увійшли в наше повсякденне життя і стали вагомою частиною соціальних контактів.

***

10.04.2018
Исследование: 16 % женщин никогда не расстаются со смартфоном

Издание AdWeek показало в инфографике, как женщины используют мобильные телефоны (Телекритика).

Смартфоны настолько укоренились в обществе, что более 60 % женщин владеют двумя или более мобильными устройствами и используют их каждый день. Почти половина женщин в возрасте от 18 до 34 лет проверяют свои телефоны как только проснутся, а еще 36 % проверяют их в течении пяти минут после пробуждения. Более того, около четырех процентов «залипают» с утра в смартфонах более чем на час.

Помимо разговоров и переписки 73 % женщин используют смартфоны для чтения новостей, 25 % расплачиваются с их помощью в магазинах, а 89 % узнают погоду.

Для 96 % женщин смартфон – это фотокамера, 81 % покупают одежду с помощью смартфона, 86 % смартфон помогает готовить еду. Большинству дам в смартфоне нужен калькулятор (88 %), будильник (84 %), календарь (83 %) и навигатор (82 %).

16 % женщин никогда не расстаются с телефоном.

Маніпулятивні технології

2.04.2018

Иран планирует заблокировать Telegram и заменить его собственным

Иранские власти планируют заблокировать Telegram к концу апреля 2018 года. Об этом пишет иранское агентство Mehr (IGate).

По словам главы комиссии по национальной безопасности Алаэддина Боруджерди, власти решили ограничить доступ к мессенджеру из-за его роли в организации протестов в стране. Место Telegram может занять созданный в Иране сервис Soroush, который запустится 20 апреля.

В декабре 2017 года власти Ирана временно ограничили доступ к Telegram и Instagram. По словам основателя сервиса Павла Дурова, мессенджер заблокировали из-за отказа компании закрыть каналы мирных протестующих.

В январе 2018 года Telegram разблокировали – по версии Reuters, из-за ограничений пострадали сотни компаний, а около 100 тысяч человек лишились работы.

***

4.04.2018

В Малайзии можно сесть в тюрьму на шесть лет за распространение фальшивых новостей

В Малайзии приняли новый закон, согласно которому граждане страны, распространяющие фальшивые новости в социальных сетях и на веб-сайтах, будут наказываться штрафом в 500 тысяч ринггитов ($123 тысячи) и возможным тюремным заключением сроком до шести лет. Закон, продвигавшийся премьер-министром Наджибом Разаком (Najib Razak), был одобрен в парламенте несмотря на то, что некоторые раскритиковали его за возможное препятствие свободе слова (InternetUA).

Изначально законопроектом за распространение фальшивых новостей предполагалось тюремное заключение сроком до 10 лет, но в итоге правительство решило остановиться на шести годах. Такими делами будет заниматься независимая судебная инстанция. Закон может распространяться и на граждан, которые находятся за пределами Малайзии, но публикуют лживые материалы о стране и её жителях.

Малазийский закон определяет фальшивые новости как «новости, информацию, данные и отчёты, частично или полностью ложные». Это могут быть текстовые материалы, а также видео- и аудиоконтент.

***

4.04.2018

Facebook представил новую антифейковую функцию. Пока только в США

В скором времени пользователи смогут отслеживать, кто из их друзей чаще всего делится фейковыми новостями (Телекритика).

Если трансформировать популярное высказывание Гиппократа под сегодняшнии реалии, то получится примерно такая фраза: «Ты – то, что ты постишь». И с этим трудно поспорить.

Вот уже несколько лет в социальных медиа и в СМИ обсуждаются вопросы фейковых новостей и низкосортного контента, которым буквально забит интернет. Этот контент постят, репостят, шэрят и твитят огромное количество пользователей. И найти среди этого информационного мусора достойную внимания публикацию порой бывает очень сложно.

Сегодня Facebook, который подвергается нападкам общественности уже несколько месяцев подряд из-за утечки личных данных юзеров, внедряет новую функцию. Аккурат в тот момент, когда основателя соцсети Марка Цукерберга хотят убрать с должности главы компании.

Благодаря новой функции соцсети каждый пользователь сможет увидеть больше информации о человеке, который запостил в своем профиле тот или иной материал. Новая функция будет применяться в основном к изданиям.Возле новости от издания появится значок i, при нажатии на который будет появляться блок с ответом из Википедии (аналогичный блоку выдачи в Google), где вы сможете узнать краткую информацию об издании.

Под постом издания также будут расположены статьи на похожие темы, так называемый related content, и список людей, которые поделились этим постом в своем профиле. Таким образом, можно будет выявлять друзей, которые делятся реальным контентом и тех, которые распространяют фейковые новости.

***

4.04.2018

Facebook удалил сотни публикаций российской «фабрики троллей»

Facebook удалил несколько сотен учетных записей, страниц и публикаций российского Агентства интернет-исследований (АИИ), известного как «фабрика троллей». Об этом глава компании Марк Цукерберг сообщил Reuters (InternetUA).

В США АИИ обвиняют во влиянии на общественное мнение американцев с помощью соцсетей во время президентской кампании в 2016 году.

Отмечается, что многие удаленные материалы опубликованы Федеральным агентством новостей (ФАН). Служба безопасности Facebook

проанализировала страницы и публикации и пришла к выводу, что ФАН технологически и структурно связано с АИИ.

По словам Цукерберга, агентство «неоднократно обманывало людей и манипулировало ими по всему миру». «Мы не хотим видеть их на Facebook где бы то ни было», – подчеркнул он.

***

7.04.2018

Facebook перевірятиме особливо популярні сторінки соцмережі

Компанія Facebook планує перевірити особливо популярні сторінки, аби перешкодити користувачам використовувати фейкові акаунти для того, щоб приховувати свою особистість (Свідок).

Про це заявив засновник мережі Марк Цукерберг, пише BBC.

Також це має допомогти у боротьбі із поширенням неправдивих новин та пропагандою.

У компанії не вирішили, що саме вважати «популярними сторінками», але додають, що буде враховуватися ціла низка параметрів, зокрема, і число підписників.

Facebook вже перевіряє, чи дійсно сторінки, створені від імені зірок або інших широко відомих людей, належать їм. Як говорить компанія, процес верифікації найбільш популярних сторінок, швидше за все, буде працювати так само.

Спецслужби і технології «соціального контролю»

2.04.2018

В Telegram объяснили невозможность предоставления ФСБ ключей шифрования

Юристы Telegram сообщили Роскомнадзору о невозможности выполнения требований ФСБ России по предоставлению ключей шифрования. Об этом сообщает РИА «Новости» со ссылкой на юриста компании Дмитрия Динзе (InternetUA).

«Администратор сервиса в существующей архитектуре ни при каких условиях не имеет доступа к информации, дающей возможность декодирования принимаемых, передаваемых, доставляемых и обрабатываемых с его помощью электронных сообщений», – говорится в официальном заявлении Telegram.

***

2.04.2018

ФБР использует засекреченные хакерские инструменты в рядовых расследованиях

Одним из самых малоизвестных отделов ФБР США является Подразделение удаленных операций (Remote Operations Unit, ROU), занимающееся взломом компьютеров и мобильных устройств. До недавнего времени ROU в публичных документах не упоминалось, однако теперь эта аббревиатура впервые появилась в отчете Управления генерального инспектора (Office of the Inspector General, OIG) Министерства юстиции США. Более того, согласно документу, ROU использует засекреченные хакерские инструменты, предназначенные для обеспечения нацбезопасности, в рядовых уголовных расследованиях (InternetUA).

ROU является частью подразделения операционных технологий ФБР (Operational Technology Division, OTD), занимающегося технологической стороной расследований. Как сообщается в отчете OIG, ROU обладает «возможностями для эксплуатации компьютерной сети» и сотрудничает «с инженерами и поставщиками техник для эксплуатации мобильных устройств».

Отчет OIG в основном посвящен тому, что ФБР не исследовало полностью свои возможности для взлома iPhone террориста из Сан-Бернардино в 2016 году. Однако несколько разделов документа также проливают свет на деятельность ROU и использование подразделением хакерских инструментов.

Изначально ROU не участвовало в поисках решений для разблокировки iPhone террориста, поскольку инструменты для обеспечения нацбезопасности не должны использоваться в расследованиях уголовных дел. Помимо прочего, ФБР является органом разведки, в обязанности которого входит сбор данных для защиты государства, а не только для предъявления формальных обвинений подозреваемым. Тем не менее, с разрешения заместителя генерального прокурора США ФБР может использовать засекреченные техники в рядовых расследованиях, говорится в отчете.

***

4.04.2018

Профили россиян в соцсетях «Одноклассники» и «ВКонтакте» сдали кредиторам

Национальное бюро кредитных историй РФ (НБКИ), продолжит поддерживать сервис, проверяющий в социальных сетях личные странички пользователей-заемщиков.

Докладніше

***

4.04.2018

Жителя России посадили в тюрьму за одно сообщение в Telegram

Новости об уголовных делах за публикации и репосты на открытых интернет-площадках или соцсетях уже перестали нас удивлять. И вот 4 апреля

– на фоне возможной блокировки детища Павла Дурова – стало известно о первом уголовном деле за репост в мессенджере Telegram. Дело возбуждено против юриста из Приморского края Дмитрия Третьякова (InternetUA).

Как сообщает издание fontanka.ru, его обвиняют по второй части 280 статьи Уголовного кодекса Российской Федерации – публичные призывы к экстремизму с использованием интернета. В одном из сообщений Дмитрия специалисты выявили признаки призыва к насильственным, деструктивным и разрушительным действиям.

Как стало известно, Дмитрия Третьякова арестовали ещё 16 марта во Владивостоке. По решению суда, он будет находиться в СИЗО как минимум до 13 мая. В квартире подозреваемого проведены обыски. Причиной задержания стал сделанный ещё в прошлом году репост сообщения из Telegram-канала журналиста Аркадия Бабченко. Если факт нарушения закона будет установлен следствием и доказан в суде, то юристу грозит до пяти лет заключения.

***

4.04.2018

Ультиматум Роскомнадзора: Почему в России хотят заблокировать Telegram и получится ли это сделать

Четвертого апреля закончился срок действия ультиматума, выдвинутого Роскомнадзором к мессенджеру Telegram. Теперь ведомство (поскольку в Telegram не выполнили запрашиваемое) может обратиться в суд по поводу блокировки мессенджера на территории России. В самом Telegram решения о блокировке особо не опасаются, и на то есть причины.

Докладніше

***

9.04.2018

ФБР арестовало один из старейших в мире сайтов объявлений

ФБР арестовало сайт Backpage.com, который обвиняется в размещение объявлений о сексуальных услугах и рабстве. Арест был произведен на фоне принятия в США закона, по которому операторы онлайн-площадок начнут нести ответственность за содержание материалов, размещенных третьими лицами.

Докладніше

***

10.04.2018

В Китае ограничат доступ к интернету за плохое поведение

Правительство Китая следит за гражданами и назначает им уровень социального доверия, который может повлиять на многие стороны жизни, в том числе на скорость интернет-соединения (IGate).

В стране с 2014 года постепенно вводится система оценки социального доверия, в рамках которой действия граждан должны оцениваться и вознаграждаться, либо наказываться. Программа работает в пилотном режиме, для большинства жителей страны её запустят ближе к 2020 году.

В 2017 году автор WIRED Рейчел Ботсман опубликовала исследование этой системы, и сделала немало интересных открытий.

Учёт действий граждан ведут различные учреждения, от городских советов, до частных технологических компаний, у которых есть доступ к личным данным пользователей. Принцип оценки поведения до конца неизвестен – нельзя точно сказать, какие действия влияют на статус человека сильнее.

Проблема захисту даних. DDOS та вірусні атаки

28.03.2018

Вредоносы для Android скрывались под видом полезных утилит

SophosLabs предупредила о новых вредоносных программах, найденных в магазине Google Play, которые прятались под видом полезных утилит. Эксперты идентифицировали это семейство вредоносных программ как Andr/HiddnAd-AJ.

Докладніше

***

28.03.2018

Ольга Карпенко

Mozilla выпустила дополнение для Firefox, блокирующее «слежку» Facebook за пользователем

Компания Mozilla, разработчик популярного браузера Firefox, создала специальное дополнение для него, которое блокирует трекинг действий пользователя со стороны социальной сети Facebook. Дополнение бесплатно и называется Facebook Container.

Докладніше

***

28.03.2018

Вымогатель научился удалять антивирусы с компьютеров жертв

Эксперты из MalwareHunterTeam обнаружили программу-вымогатель AVCrypt, которая блокирует работу установленных на компьютере антивирусов до того, как вся информация на устройстве будет зашифрована. Об этом сообщает Bleeping Computer (InternetUA).

По словам специалистов, AVCrypt удаляет службы программного обеспечения Windows Defender и Malwarebytes. Затем вымогатель запрашивает у системы информацию о других антивирусах, зарегистрированных в Центре обеспечения безопасности Windows, после чего пытается избавиться и от них через командную строку. При этом данный способ почему-то не работает с программой Emsisoft.

Исследователи в области информационной безопасности отмечают, что никогда раньше не фиксировали деятельность вымогателей такого рода. Они также предположили, что вирус может являться программой-вайпером, то есть создан для уничтожения информации на устройстве жертвы.

Специалисты отметили, что злоумышленники не оставили контактные данные для отправки выкупа. Вместо этого в записке с требованиями они написали «lol n».

***

28.03.2018

Хакерская группировка Cobalt продолжает атаковать банки

Исследователи безопасности из компании Group-IB зафиксировали новую кибератаку хакерской группировки Cobalt, также известной как Carbanak и Anunak. Хакеры продолжают проявлять активность даже после ареста человека, предположительно являющегося лидером группировки.

Докладніше

***

29.03.2018

Уязвимость сети: как защитить свои данные в интернете

Данные 50 млн человек попали в чужие руки. Эксперты: нужно настроить соцсети и пользоваться VPN.

Докладніше

***

1.04.2018

Хакеры украли данные 150 млн пользователей спортивного приложения от Under Armor

Компания Under Armor, которая разрабатывает приложение MyFitnessPal, сообщила, что в конце февраля 2018 года стала жертвой хакерской атаки.

Злоумышленники украли данные 150 млн пользователей, сообщает MacRumors (IGate).

Хакеры смогли получить данные, которые включают имена пользователей, электронную почту и зашифрованные пароли. Информация о банковских картах, которые были привязаны к аккаунту, не пострадали.

Under Armor уже отправляет письма и уведомления в приложении своим клиентам, которые пострадали из-за действий хакеров. Всем пользователям MyFitnessPal рекомендуется сменить пароль от аккаунта. Компания заявила, что работает с полицией и ведущими фирмами по защите данных, чтобы быстрее расследовать дело и найти виновных.

MyFitnessPal – одно из самых популярных приложений в категории «Здоровье и фитнес». Кураторы App Store не раз называли его одним из лучшим в своей категории. MyFitnessPal позволяет пользователям следить за количеством потребляемых калорий. В приложении есть база из двух миллионов продуктов.

***

2.04.2018

Хакеры украли данные 5 млн банковских карт

Хакеры из группировки Fin7, также известной под названием JokerStash, выкрали данные кредитных карт более чем пяти миллионов американцев. Как сообщает компания Gemini Advisory, информация о 125 тысячах карт выставлена на продажу, оставшиеся данные также могут в скором времени быть раскрыты (InternetUA).

Под удар попали клиенты магазинов Saks Fifth Avenue и Lord & Taylor, совершавшие покупки в период с мая 2017 года по настоящее время. Большинство пострадавших проживают в штатах Нью-Йорк и Нью-Джерси.

С заявленным количеством скомпрометированных платежных карт, нынешняя хакерская атака является одной из самых больших и наиболее вредных для сферы ретейла, – утверждают специалисты в области кибербезопасности.

Ранее эта группировка взломала базы клиентов сетевых магазинов Whole Foods, Chipotle, а также отелей Omni Hotels & Resorts и Trump Hotels.

***

2.04.2018

Acronis: более 40 % пользователей никогда не слышали о вредоносах-вымогателях

Ежегодно Acronis проводит глобальный опрос потребителей, который приурочен к Всемирному дню резервного копирования (World Backup Day), чтобы оценить отношение, привычки и знания общественности касательно защиты данных.

Докладніше

***

3.04.2018

Хакер зламував сторінки у соцмережах і вимагав гроші за відновлення

За допомогою фішингу киянин відбирав у власників доступ до їх персональних сторінок, після чого вимагав за нього гроші. Такі дії зловмисника кваліфіковані поліцією за двома статтями Кримінального кодексу України.

Докладніше

***

3.04.2018

Витік даних Facebook: Цукерберг зізнався, що на вирішення проблем з безпекою підуть роки

Для вирішення проблем соціальної мережі Facebook у сфері безпеки знадобиться кілька років (Espreso.tv).

Про це заявив очільник компанії Марк Цукерберг в інтерв'ю виданню Vox.

Він зауважив, що протягом перших 10 років роботи компанії всі були зосереджені на позитивних її аспектах. А от тепер люди вже почали звертати увагу на деякі ризики і недоліки.

За його словами, керівництво Facebook занадто повільно інвестувало деякі речі, зокрема безпеку. Цукерберг пригадав, що на початку минулого року у штабі компанії було 10 тисяч людей, які працювали у сфері безпеки. А от наприкінці цього року їхня кількість має зрости вдвічі.

«З точки зору вирішення багатьох з цих проблем, я думаю, що це просто випадок, коли ми недостатньо інвестували, я думаю, що ми прорвемося, але на це піде кілька років. Хотів би я вирішити всі ці проблеми через три місяці або шість місяців, але я просто думаю, що реальність полягає в тому, що на рішення деяких з цих питань піде набагато більше часу», – наголосив Цукерберг.

***

3.04.2018

Facebook случайно хранила удаленные пользовательские видео

Беда не приходит одна, в чем в очередной раз убедилась социальная сеть Facebook. Вернее, определенные неурядицы случаются с компаниями постоянно, однако внимание к происходящему может быть разным. В случае с детищем Марка Цукерберга каждый неверный шаг соцсети расценивается почти как трагедия и живо обсуждается в сети (InternetUA).

На прошлой неделе выяснилось, что Facebook хранила на серверах пользовательские видео, которые были ими удалены и не предназначались для публикации на страницах сервиса. Речь идет о роликах, снятых тогда, когда соцсеть позволяла записывать их на собственные мощности социальной сети.

Спустя примерно неделю в Facebook разобрались, в чем же проблема. Она, как оказалось, кроется в «баге». Социальная сеть также принесла свои извинения.

***

3.04.2018

Михаил Сапитон

Google Chrome сканирует пользовательские файлы на Windows. Это не опасно

Браузер Google Chrome, рыночная доля которого перевалила за 60 %, подвергся нападкам ряда пользователей Twitter. Они обнаружили, что браузер сканирует их компьютеры на Windows. Проверке подвергаются, в том числе, и документы из пользовательских папок, не связанных с системными функциями или установкой софта.

Докладніше

***

4.04.2018

Обнаружен ворующий переписку в мессенджерах вирус

Исследователи корпорации Trustlook Labs обнаружили троян для Android, который способен украсть данные практически из всех известных сервисов обмена сообщениями. Об этом сообщается в блоге компании (InternetUA).

По данным специалистов, вирус не позволяет системе проанализировать свой код и способен обойти антивирусную защиту.

Вредоносное программное обеспечение изучает данные мобильных клиентов Telegram, Viber, Facebook Messenger, Skype, Line и других мессенджеров. Эксперты утверждают, что алгоритм вируса выстроен таким образом, чтобы автоматически отсылать данные на удаленный сервер: скорее всего, захваченные массивы могут использоваться для шантажа жертв и получения выкупа.

Специалисты по кибербезопасности обнаружили вредоносное программное обеспечение в китайском приложении Cloud Module. Пакет, хранящий троян, назывался com.android.boxa. Скорее всего, он распространяется через сторонние магазины приложений для Android и ссылки, публикуемые злоумышленниками.

***

4.04.2018

Обнаружено российское приложение, которое собирает данные украинских военных

Украинских военных предостерегают от использования российского мобильного приложения, которое собирает персональную информацию и отслеживает передвижения пользователей (InternetUA).

Об этом сообщает Главком со ссылкой на Военное телевидение.

Отмечается, что таких шпионских программ, которые могут иметь доступ к почти всем данным на мобильных устройствах, несколько. Но все они имеют единое общее – это российское происхождение. Наиболее популярным, считают эксперты, является «ДМБ Таймер».

«На первый взгляд, это бесплатная программа, которая считает количество дней до окончания службы. На самом деле, это – находка для врага», – констатируют военные журналисты.

В частности, это приложение получает информацию об активности пользователя, который использует на своем мобильном устройстве службу геолокации, камеру, микрофон, внутреннюю память. Также программа может блокировать спящий режим телефона.

Как обнаружили через социальные сети авторы сюжета, пользователями российского шпионского приложения являются многие украинские военнослужащие, в том числе и участники боевых действий.

«Мобильные приложения стали полноценным оружием во время гибридной агрессии РФ. И, к сожалению, это оружие эффективно и не требует привлечения больших средств», – отмечает военное телевидение.

***

4.04.2018

Игра для Android скрытно подписывала пользователей на платный сервис

Специалисты ESET обнаружили новую мошенническую схему. Приложение Pingu Cleans Up подписывало пользователей на дорогостоящий сервис, используя легитимный способ оплаты в Google Play.

Докладніше

***

4.04.2018

Google исправила более 300 уязвимостей в ОС Android

Компания Google выпустила обновление для операционной системы Android, исправляющее в общей сложности 312 уязвимостей, из которых 9 являются критическими и позволяют злоумышленнику удаленно выполнить произвольный код. При этом 287 проблемам была присвоена высокая степень опасности.

Докладніше

***

5.04.2018

Facebook сообщила об утечке данных 87 млн пользователей в скандале с Cambridge Analytica

Facebook уточнила число пользователей, пострадавших от утечки данных с участием Cambridge Analytica: их количество увеличилось с 50 млн до 87 млн человек (IGate).

Социальная сеть предупредит пострадавших пользователей, отправив им уведомление о том, какие их данные получила Cambridge Analytica. Пользователи увидят уведомление в верхней части новостной ленты Facebook, в нём также будут перечислены все приложения, использующие личные данные. Пользователи смогут удалить эти приложения.

***

5.04.2018

Пользователи WhatsApp оказались в опасности

Специалисты обнаружили, что данные участников групповых чатов в мессенджере WhatsApp находятся под угрозой, поскольку любой желающий может собрать их в базу, включающую номера мобильных телефонов пользователей, а также изображения, видео и ссылки, которыми они делились в чате. Об этом сообщает Venture Beat (InternetUA).

Исследование провели Киран Гаримелла (Kiran Garimella) из Федеральной политехнической школы в Лозанне и Гарет Тайсон (Gareth Tyson) из Лондонского университета королевы Марии. Специалисты в течение полугода собирали информацию из 178 групповых чатов, которые они обнаружили с помощью веб-поиска. Всего было проанализировано полмиллиона сообщений, отправленных почти 46 тысячами пользователей.

Гаримелла и Тайсон использовали смартфон, на который был установлен WhatsApp, и применили метод расшифровки данных, предложенный индийскими специалистами. Вся информация, полученная из чатов, хранится в локальной базе данных на устройстве, как и ключ дешифрования. Они смогли извлечь его и получили массив данных групп.

В исследовании также говорится, что информация может быть собрана только после вступления в групповой чат, ранее отправленные сообщения при этом будут недоступны.

***

9.04.2018

YouTube обвинили в шпионаже за детьми

В США члены правозащитных организаций направили в Федеральную торговую комиссию жалобу на видеохостинг YouTube, передает CNN (InternetUA).

Как сообщается, дочернюю компанию Google обвиняют в незаконном сборе информации о лицах младше 13 лет. Таким образом нарушается закон о защите конфиденциальности детей в интернете (Children's Online Privacy Protection Act – COPPA): YouTube собирает конфиденциальную информацию о подписчиках каналов, в том числе о детях, не получая на это согласия их родителей. В поданной в комиссию жалобе отмечается, что за несколько лет были нарушены права более 23 млн детей. Кроме того, выдвинуто требование оштрафовать Google по меньшей мене на $41 млн.

«Google получает большие прибыли от сбора и использования персональных данных о детях на YouTube. Этот незаконный сбор происходит уже много лет и охватывает десятки миллионов детей в США», – говорится в жалобе.

***

10.04.2018

Миллионы пользователей Android стали жертвами антивирусов-имитаторов

Почти семь миллионов человек стали жертвами ложных антивирусов, размещенных мошенниками в каталоге Google Play, пишет WeLiveSecurity со ссылкой на отчет вирусных аналитиков ESET. В общей сложности специалистами компании было выявлено 35 приложений, имитирующих функциональность программ по обеспечению защиты устройств на базе ОС Android от вредоносного ПО (InternetUA).

К счастью пользователей, приложения-подделки не содержали вредоносного кода, лишь имитируя активную борьбу с вирусными программами. Некоторые из ложных антивирусов и вправду сканировали устройства пользователей, без разбору нарекая статусом вредоносных вполне безобидные программы. Как правило, вредоносными признавались приложения, имеющие доступ к SMS-сообщениям и адресной книге.

К числу вредоносных такие «антивирусы» также относили и себе подобные программы. Их создатели, не желая терять аудиторию просматривающих рекламу пользователей, требовали от них безотлагательно удалить антивирусное приложение, дублирующее функциональность уже установленного. На момент выхода публикации все имитаторы из списка ESET были удалены цензорами Google Play.

ДОДАТКИ

Додаток 1

1.04.2018

Facebook требовал от сотрудников увеличения аудитории любой ценой

Один из наиболее влиятельных менеджеров Facebook Эндрю Бозворт, известный как Боз, рекомендовал своим сотрудникам использовать любые методы, если они помогают увеличить аудиторию соцсети, следует из его письма подчиненным, опубликованного Buzzfeed (InternetUA).

Документ, который называется The Ugly (Уродливое) был написан Бозвортом в июне 2016 года, когда президентская кампания, важную роль в которой сыграл Facebook, в США подходила к своему завершению.

Сотрудники компании получили письмо на следующий день после убийства мужчины в Чикаго, которое убийца транслировал в Facebook в прямом эфире и, очевидно, письмо было реакцией на это событие.

Бозворт отмечает, что данные, которые люди получают из Facebook, действительно могут быть использованы не во благо, однако это не имеет значения, если новые методы позволяют людям еще быстрее находить друг друга.

«Уродливая правда в том, что мы верим в соединение людей так глубоко, что все, что позволяет нам еще больше людей еще чаще “де факто” хорошо. Возможно, это единственная область, где метрика действительно говорит нам правду о том, чем мы занимаемся,– написал Бозворт. – Это не то, что мы делаем для себя или для цены наших акций (ха!). Это именно то, что мы делаем. Мы соединяем людей. Точка».

Эндрю Бозворт уже прореагировал на публикацию Buzzfeed, опубликовав комментарий в Twitter.

«Я не согласен с этими утверждениями сейчас, и даже не был согласен с ними, когда их написал,– отметил он. – Спорить на подобные жесткие темы – важная часть нашего процесса. И чтобы сделать это эффективно, мы должны быть готовы принимать даже плохие идеи, но только в случае, если устранять их».

Эндрю Бозворт пришел в Facebook из Microsoft в 2006 году. Наравне с Марком Цукербергом он входит в узкий круг сотрудников, вовлеченных во все процессы компании. За годы своей работы он успел поучаствовать в разработке групп и новостных лент, а также системы по борьбы со злоупотреблениями. В настоящий момент Бозворт занимает должность вице-президента по дополненной и виртуальной реальности.

(вгору)

Додаток 2

2.04.2018

Михаил Сапитон

Opendatabot запустил уведомления о судебных делах через мессенджеры

Проект Opendatabot запустил возможность удаленно узнавать об открытии и обновлении статуса судебных дел. Для этого нужно найти в боте (доступен для Skype, Telegram, Facebook и Viber) свою компанию или ФЛП, выбрать опцию «Поиск в судебных делах» и подписаться. Как только в судебном реестре появятся новые материалы, пользователь получит нотификацию. Ранее требовалось вручную проверять ход дела, а самостоятельно узнать об его открытии без получения письменного уведомления было практически нереально (AIN.UA).

Инициатива призвана покончить с ситуациями, когда предприниматель или компания, являясь фигурантами судебного дела, даже не догадываются о его развитии. Причина чаще всего скрывается в доставке судебных повесток: многие люди не проживают по адресу прописки, а письма могут затеряться или вручить кому-то другому. При этом доказать, что повестку вы не получили, получится лишь после вынесения судебного решения или на следующем заседании.

Opendatabot приводят два громких случая, когда отсутствие уведомлений о судебных делах повлекли серьезные последствия. Первый – ситуация вокруг завода «Крымсода», принадлежащий украинскому бизнесмену Дмитрию Фирташу. В 2015 году киевский Хозяйственный суд взыскал с предприятия масштабный кредит в пользу компании-однодневки ООО «Юг Сода», зарегистрированной в заброшенном подмосковном доме. Сумма задолженности, которую «Юг Сода» выкупила за 150 млн руб, составила 1,2 млрд руб. Второй пример – арест имущества «Укртелефильма» компанией «Эверест», которое состоялось благодаря заочному решению судьи днепропетровского Индустриального районного суда.

(вгору)

Додаток 3

9.04.2018

Флешмоб: жители Киева назвали самые опасные ТРЦ

Киевляне в социальных сетях объявили флешмоб #проверьторговыйцентр на предмет пожарной безопасности и начали выкладывать в Facebook свои наблюдения, сопровождая их фото. Также свои проверки начали и в ГСЧС (Вероятно).

«Вести» собрали «народный рейтинг» самых проблемных ТРЦ, в которых были замечены нарушения.

Издание отмечает, что после пожара в кемеровском ТРЦ, когда в огне погибли 64 человека, киевляне в соцсетях объявили флешмоб, предлагая самим подписчикам проверить все торговые центры, снять на видео и выложить в Facebook, где какие проблемы, открыты ли все двери, есть ли планы эвакуации, имеется ли противопожарная сигнализация и т. д. (в Кемерово была отключена

сигнализация, оповещающая о задымлении, были закрыты эвакуационные выходы, и люди хаотично пытались спастись сами).

Судя по сообщениям киевлян, не все столичные ТРЦ ликвидировали свои нарушения правил пожарной безопасности. По наблюдениям участников флешмоба, почти во всех ТРЦ пожарные выходы оказались закрытыми, а во многих местах их вообще не видно за раскладками товаров, которые расположили прямо на пути эвакуации. Также в отдельных центрах и вовсе отсутствовали элементарные указатели к эвакуационным выходам.

Так, к примеру, в «Магелане» во время проверки на одном из эвакуационных выходов расположился ресторан, другие выходы на этажах были завалены хламом или закрыты на замок. Киевлянам удалось найти только одну дверь, через которую можно выйти. Правда, как сообщили в администрации ТРЦ, все нарушения уже были устранены, а проверку «Магелана» начала ГСЧС .

Стоит отметить, что размещение кафе и магазинов на пожарных проходах и выходах является распространенным нарушением в столичных центрах. Кроме «Магелана» такое нарушение было зафиксировано в «Олимпийском» и «Караване». К слову, в последнем также отсутствовала общая схема эвакуации на случай ЧП. В «Олимпийском» комментировать ситуацию отказались, а в «Караване» целый день не брали трубку.

(вгору)

Додаток 4

6.04.2018

#РозкажиЯк: у мережі набирає обертів флешмоб про успішні приклади громадської активності

Під хештегом #РозкажиЯк активісти з різних міст України у соцмережах поширюють історії про те, як своїми діями змінюють громаду та спонукають громадян брати відповідальність за своє оточення (Вчасно).

Флешмоб розпочали активісти руху «Сильні громади», аби показати, що стара модель очікування на зміни та покладання надій на владу не працює.

За словами координатора руху «Сильні громади» Валентина Краснопьорова, людям потрібно показувати на прикладах, що варто самим брати відповідальність і змінювати свої громади.

Флешмоб вже охопив активістів з понад півтора десятка міст Донеччини, Луганщини та Дніпропетровщини, а загальна кількість історій складає вже більше 40. Наразі в мережі опубліковані історії активістів із понад 15 міст.

Так, Дмитро Макуха з селища Билбасівка Слов'янського району розповів історію про те, як об'єднавши зусилля з друзями, вдалося привести до ладу селищний парк та ініціювати встановлення урн.

Олександр Цахнів із Селидового розповів, як у невеликому місті на Донеччині юні активісти відроджують українські народні традиції і проводять театралізоване святкове дійство – Різдвяний вертеп.

Також Олександр розповів, як Селидівська громада відстояла тарифи на воду.

Активістка з Бахмуту Олена Щекодіна розповіла історію про згуртування людей навколо прибирання пляжу, до якого долучилися не лише учасники акції, але люди, що відпочивали на пляжі.

Активістка зі Слов'янська Євгенія Калугіна поділилася історією про те, як її пост про зношені сидіння в маршрутних автобусах міста отримав широкий суспільний резонанс, спровокував дискусію в соцмережах. Власник маршрутки відреагував на критику та змінив обшивку сидінь.

У Дружківці люди об'єдналися в ініціативну групу, щоб боротися зі свавільними відключеннями водопостачання в літню спеку. Кому ці відключення могли бути вигідні і як містянам вдалося вплинути на вирішення проблеми – про це розповів Павло Островський.

У Сєвєродонецьку активісти домоглися якісного ремонту дороги на одній із вулиць міста.

Більше історій можна прочитати в мережі Фейсбук за хештегом #РозкажиЯк.

Активісти руху «Сильні громади» закликають долучатися до флешмобу та розповідати про власні приклади активностей, що згуртували громаду. Для цього варто просто розповісти історію, яка надихає і може надихнути інших і додати хештег #РозкажиЯк.

(вгору)

Додаток 5

5.04.2018

У мережі набирає обертів флешмоб у підтримку Уляни Супрун

Владика Ірина

На просторах Інтернету розпочався флешмоб #япідтримуюсупрун. Таким чином, деякі інтернет-користувачі засуджують можливе звільнення Уляни Супрун з посади виконувача обов'язків міністра охорони здоров'я.

Приєднались до акції й кілька громадських активістів із Івано-Франківська: Михайло Джогола та Олег Паньків. Вони вже встигли викласти власне фото із відповідним підписом у соцмережах (Місто).

Нагадаємо, кілька днів тому комітет Верховної Ради з питань охорони здоров'я схвалив проект звернення до Кабміну щодо звільнення Супрун з посади та висловив їй недовіру.

На думку членів комітету, Супрун викликає гостру суспільну напругу через зрив програми державних закупівель ліків у 2016 році.

Підтримала проект й депутат Ольга Богомолець, про це вона повідомила на своїй сторінці у соцмережі.

«Я підтримала проект постанови, але хочу зауважити, що приводів для звільнення – набагато більше, і треба розібратися, що стало причиною катастрофи в медицині – професійна непридатність в. о. міністра чи свідома

урядова політика, адже роботу уряду в частині охорони здоров'я також було визнано Комітетом незадовільною», – йдеться у повідомленні Богомолець.

Також вона вказала особистий перелік претензій до роботи керівництва МОЗ. Серед основних звинувачень – прискорення темпів вимирання українців, «відтік» медиків за кордон, спад рівня вакцинації населення, зірвані міжнародні закупівлі ліків, мізерна оплата праці медичних працівників, провал програми боротьби з раком. Крім цього, лікування онкологічних та серцево-судинних захворювань, що разом спричиняють 80 % усіх смертей – профінансовано лише на 27 % та 30 % відповідно.

«Все це – неповна картина тієї катастрофи, до якої привело нас всього за два останні роки керівництво МОЗ. Відставка – це найменше, що потрібно зробити в даній ситуації. Мають бути ще й кримінальні справи, розслідування та терміни ув'язнення за знищення системи охорони здоров'я України та її людського потенціалу», – додає Богомолець.

(вгору)

Додаток 6

9.04.2018

Соцсеть исправляется: как Facebook защитит данные пользователей

Из-за скандала, разгоревшегося вокруг политики конфиденциальности Facebook, руководство социальной сети решило ограничить объем данных пользователей, предоставляемых компаниям вроде Cambridge Analytica (InternetUA).

Руководство компании Facebook заявило о закрытии функции для создания таргетированной рекламы под названием «Партнерские категории». Они позволяли маркетинговым компаниям, занимающимся обработкой и продажей данных, присылать рекламу своих клиентов определенным группам пользователей. Вот уже несколько лет такие сторонние поставщики данных, как Acxiom, Epsilon Data Management и Data Cloud (дочерняя компания Oracle), к примеру, собирают информацию о покупках пользователей и, основываясь на ней, присылают им определенную рекламу. Кроме того, эту рекламу показывают и пользователям с похожими аккаунтами. Такая смена политики компании Facebook запретит им создавать таргетированную рекламу. Представители Acxiom уже заявили, что данное изменение может сократить доходы и чистую прибыль компании в 2019 финансовом году на $25 млн.

Вице-президент компании Facebook по глобальным маркетинговым решениям Кэролин Эверсон в обращении к компаниям-поставщикам данных заявила, что изменения вступят в силу в течение полугода. Facebook, однако, не запрещает размещать таргетированную рекламу, которая стала движущей силой огромного рекламного бизнеса социальной сети. Тем не менее, по словам Кэролин Эверсон, маркетинговые компании смогут оперировать только теми данными пользователей, на использование которых у них есть «права, разрешения и законные основания». Изменения, вероятно, больше всего

затронут компании по производству потребительских товаров, в клиентских базах которых недостаточно информации.

По некоторым сообщениям, Facebook также больше не будет предоставлять сторонним поставщикам анонимизированные данные пользователей, которые позволяют таким компаниям, как Acxiom, оценить успешность проводимых ими рекламных кампаний. В среду директор по продуктовому маркетингу компании Facebook Грэм Мадд в пресс-релизе заявил, что такие изменения повысят уровень конфиденциальности данных пользователей социальной сети. В результате скандала вокруг британской аналитической компании Cambridge Analytica, которая незаконно использовала данные миллионов пользователей Facebook, как руководство Facebook, так и такие правительственные органы, как Федеральная торговая комиссия США, проверяют политику конфиденциальности сети. Компания Cambridge Analytica, получившая личные данные пользователей без их согласия, сотрудничала с президентом США Дональдом Трампом во время проведения его предвыборной кампании.

Новые настройки конфиденциальности

Помимо изменений в политике конфиденциальности компании, которые скажутся на рекламодателях, руководство Facebook также представило новые настройки конфиденциальности, которые облегчат пользователям управление их персональными данными. Создатель и CEO социальной сети Марк Цукерберг в публикации в Facebook заявил, что компания ввела новый раздел меню управления аккаунтом, в котором все настройки конфиденциальности и безопасности пользователей будут доступны в одном месте.

Теперь благодаря новому пункту меню можно добавить двухфакторную идентификацию, чтобы дополнительно защитить свой профиль. С помощью настройки «Доступ к информации» можно будет просматривать и удалять публикуемые записи, ответы на публикации других пользователей, поисковые запросы и заявки на добавление в друзья. Кроме того, можно будет управлять данными, которые Facebook использует для таргетированной рекламы, и ограничивать доступ других пользователей к публикациям и личной информации аккаунта. Скачивать данные, которыми пользователи делились на Facebook, станет гораздо легче. В эту категорию входят фотографии, публикации и контакты. Кроме того, эти данные можно будет скопировать или перенести на другое устройство.

Нововведения есть и в новостной ленте. Отныне в окне над ней будут показаны все приложения, в которых пользователи зарегистрировались с помощью аккаунта Facebook. Таким образом, пользователи социальной сети с легкостью смогут удалить приложения, привязанные к их учетным записям в Facebook. По словам руководства компании, данные изменения вступят в силу через пару недель. Компания также планирует в ближайшие несколько недель обновить используемые ею в меню термины, чтобы сделать настройки более понятными для пользователей.

В публикации на Facebook, в которой были анонсированы грядущие изменения, Марк Цукерберг заявил: «Многие из вас спрашивают, как управлять тем, какой именно информацией вы делитесь в Facebook, у кого есть доступ к ней и как ее удалить». В публикации в среду руководство компании заявило, что пользователи «активно и недвусмысленно» жаловались на то, что настройки конфиденциальности трудно найти, а также на то, что они слишком сложны для понимания. Руководство Facebook отметило, что программисты компании уже «некоторое время» работали над большей частью обновлений, а скандал вокруг Cambridge Analytica и утечки данных лишь «усилил их важность».

На прошлой неделе Марк Цукерберг огласил планы компании на ближайшее время по решению проблемы утечки данных с участием Cambridge Analytica. Эти планы включают в себя и введенные апреля обновленные настройки конфиденциальности. По словам Цукерберга, в будущем Facebook проведет тщательную проверку всех сторонних приложений, у которых был доступ к «большим объемам информации» до изменения политики компании в области данных в 2014 году. Facebook проверит все приложения «с подозрительной активностью» и запретит продолжать деятельность разработчикам, которые откажутся от проведения такой проверки. Если Facebook придет к выводу, что разработчики приложения допустили утечку личных данных, компания отстранит их от дальнейшей деятельности и предупредит всех пользователей, данные которых могли быть затронуты, в том числе и пользователей, пострадавших в скандале с Cambridge Analytica. Руководство Cambridge Analytica заявило, что данные пользователей, полученные без их разрешения, были удалены. Тем не менее, ранее в марте газеты The Guardian и The New York Times, а также телеканал Channel 4 заявили, что компания Cambridge Analytica, «возможно», все же не удалила эти данные.

На прошлой неделе руководство Facebook также заявило, что в дальнейшем существеннее ограничит доступ разработчиков приложений к данным пользователей. Компания закроет доступ разработчиков к данным, если приложение не использовалось в течение трех месяцев. Также Facebook ограничит объем данных, которые пользователи передают разработчикам приложений, когда регистрируются в них, только до имени и фамилии, фотографии профиля и адреса электронной почты. Разработчикам приложений также нужно будет получить согласие пользователей и подписать контракт с Facebook, чтобы запрашивать у пользователей доступ к их публикациям или личной информации.

(вгору)

Додаток 7

31.03.2018
Чудовища в Сети: как защититься от троллей?
Валентина Развилова

Среди интернет-комментаторов есть совершенно особенная порода людей, единственная цель которых – вывести из себя собеседника (UaInfo). Их называют троллями. Зачем они так себя ведут и как с ними общаться?

Что побуждает некоторых пользователей интернета нападать на других комментаторов? Социальный психолог Эрин Баккелс из Университета Манитобы и ее коллеги решили найти ответ на этот вопрос. Исследователи выявили значимые соотношения между склонностью к троллингу и чертами характера, составляющими «Темный квадрат». Вот эти черты:

– макиавеллизм – желание манипулировать другими и мошенничать;
– нарциссизм – крайний эгоизм, одержимость собственной персоной;
– психопатия – недостаток сострадания и эмпатии;
– садизм – удовольствие от чужих страданий.

Ученые также установили связь между сторонами «Темного квадрата» (кроме нарциссизма) и суммарным временем, которое индивид в течение дня тратит на комментарии в интернете. В ходе исследования троллей распознавали несколькими способами.

Первый способ – оффлайн-опрос о том, что респондентам больше всего нравится делать на сайтах, где можно комментировать онлайн. Участникам предложили пять вариантов ответа:

– обсуждать статьи, которые для вас важны;
– болтать с другими;
– заводить новых друзей;
– троллить;
– другое.

Второй способ – онлайн-опрос, в который включены были вопросы о троллинге и других видах поведения в интернете. Некоторые из выбранных ответов указывают на:

– прямой садизм («Мне нравится причинять людям боль»);
– косвенный садизм («Мне нравятся реалистичные струи крови в видеоиграх»);
– психопатию («Ответы должны быть быстрыми и мерзкими»);
– макиавеллизм («Неумно рассказывать свои секреты»);
– нарциссизм («Меня сравнивали со знаменитостями»).

Только 5,6 % участников опроса отметили, что им нравится «троллить». Для сравнения, 41,3 % пользователей Сети – «не-комментаторы», то есть они вообще не проявляют активности онлайн. Так что тролли, как обычно и предполагают, составляют меньшинство онлайн-комментаторов и даже меньшинство среди общего числа пользователей интернета.

Кто чаще всего становится троллями?

Чтобы понять, почему троллинг так привлекателен для личностей этого типа, ученые создали собственный инструмент исследования, который назвали «Глобальная разверстка интернет-троллинга» (the Global Assessment of Internet Trolling, or GAIT). Он содержит следующие утверждения:

– «Я давал ссылки на шокирующие сайты просто для прикола».
– «Мне нравится троллить людей на форумах или в комментариях».
– «Мне нравится портить игру другим участникам онлайн-игр».
– «Чем красивее и чище вещь, тем приятнее ее испортить».

Да, некоторые соглашаются с этими утверждениями. И опять же, такое поведение коррелирует с разнообразными формами садизма, психопатией или маккиавелизмом.

Исследователи установили соотношение между троллингом и садизмом: садисты часто становятся троллями, поскольку получают удовольствие, доставляя другим неприятности. «Как тролли, так и садисты испытывают садистическую радость, причиняя вред другим, – говорит Эрин Баккелс. – Садисты просто хотят позабавиться… и интернет для них – игровая площадка!»

Многие интернет-ресурсы, например, YouTube, принимают меры против троллей: в частности, отключают комментарии или включают премодерацию. Однако Баккелс не уверена, что эти меры действенны: «Нелегко придется модераторам, которые пытаются сдержать троллей с помощью наказаний (например, забанивая их), потому что для садистов троллинг – внутренне мотивированное поведение. В конечном счете троллинг может быть слишком привлекательным для садистов, чьи возможности выразить свои наклонности в социально приемлемом виде весьма ограничены».

Почему их называют троллями?

Есть две версии происхождения этого названия применительно к сетевым провокаторам. Первая – оно заимствовано из скандинавских мифов и сказок, в которых тролль – сверхъестественное существо, обладающее дурным нравом и отталкивающей внешностью.

Вторая версия возводит его к английскому глаголу «to trawl», который означает «ловить сетью». Тролль «ловит внимание», в котором нуждается так сильно, что готов наслаждаться гневом и отвращением, которые он вызывает у других участников.

Как узнать тролля

Чтобы сразу распознать провокатора и тем самым сохранить душевное равновесие, полезно знать некоторые приемы, которые используют сетевые тролли. Так, тролль:

– высказывает мнение, которое заведомо противоречит тому, что уже написано в комментариях до него;
– высказывается не по существу;
– перевирает ваши слова и приписывает вам то, чего вы не говорили;
– превратно толкует ваши намерения;
– переходит на личности, указывает вам на ваши недостатки;
– использует ненормативную лексику, оскорбления;
– старается показать свое превосходство;
– игнорирует любые разумные доводы.

Как вести себя с троллями

Если из-за замечания в Сети у вас:

– перехватывает дыхание,
– наворачиваются слезы,
– учащается сердцебиение,
– если вы внезапно испытываете гнев, отвращение, возмущение, полную растерянность, бессильную ярость,

велика вероятность, что это замечание сделано в порядке троллинга – целенаправленной провокации.

Если это возможно, тролля следует сразу же забанить. Если забанить невозможно, единственное разумное действие в ответ – полностью игнорировать его комментарии и не вступать с ним в общение. Проблема в том, что эмоции «зашкаливают» и требуют выхода. Однако эффективнее всего разрешать их не в Сети, а офлайн – используя техники борьбы со стрессом.

(вгору)

Додаток 8

3.04.2018

Не перетворюйтеся на пластик: черкащанка розповіла як реагувати на хейтерство та тролінг у соцмережах

Що робити з «тролями» та «хейтерами», чи видаляти незручні запитання і коментарі та чи варто розділяти «себе-людину» та «себе-професіонала», розповідає Олена Литвинова, черкащанка, яка заробляє блогерством на життя, пише in.ck.ua.

Спілкуйтеся онлайн так само, як і в реальному житті

Є люди, які вважають інтернет-простір полем вседозволеності, оскільки через монітор не можна ні «доплюнути», ні ляпаса дати. Та навіть якщо ви ніколи не зустрінете опонента в житті – таке спілкування бачать інші. Я якось відмовилася брати людину на роботу через її агресивну відповідь на цілком коректний коментар іншому користувачу в Facebook. Зрозуміла, що не спрацюємося.

Відрізняйте конструктивну критику від «тролінгу» та «хейтерства»

Під час невербального спілкування легко неправильно зрозуміти співрозмовника, опираючись лише на текст – без міміки, жестів, інтонації. Якось під моїм постом про допомогу тваринам «випадковий Facebook-перехожий» написав, що я неправильно поширюю інформацію. Я уїдливо відповіла: «То навчіть, як треба». Несподівано чоловік прислав мені в «приват» масу корисної інформації, посилань, а переконавшись, що я дійсно волонтер, ще й забезпечив притулок кормом на декілька місяців.

Не дозволяйте топтатися брудними чобітьми у своєму домі

Facebook-сторінка – це, по суті, віртуальна домівка, тож гостей слід приймати аналогічно. Якщо людина починає з грубощів, образ, недоречних зауважень, не лише до власника сторінки, а й до його друзів, учасників дискусії, то чи варто терпіти цього хама у власному інформаційному просторі? Звісно, не слід влаштовувати з оточення у соцмережі «теплу ванну» з суцільних

прихильників, бо можна зовсім «відірватися від реальності». Просто лишайте тих, чия критика допомагає вам «рости», і блокуйте тих, хто прагне самоствердитися через вас.

Не видаляйте пости, коментарі та незручні питання. Особливо на бізнес-сторінках

Рукописи не горять, тим паче не горять скріншоти, тож опонент матиме ще одного «козиря» – видалили, отже, щось приховуєте. Завжди можна знайти спокійну адекватну відповідь або запропонувати перевести дискусію в формат приватних повідомлень чи особистої зустрічі.

Перевіряйте інформацію за першоджерелом

Не піддавайтеся на істерії в соцмережах, коли люди масово репостять новини кількарічної давності чи інформаційні «вкиди» з фейкових акаунтів. Хоча б «загугліть» новину та фото, подивіться, скільки друзів і підписників має людина, яка поширює неймовірні дані. Якщо інформацію не вдається перевірити, почекайте декілька годин. Хтось неодмінно це зробить і викладе результати.

Не влазьте в «бійку» під чужим постом

Краще створіть власний контент. Залишаючи низку коментарів під чужим постом, ви щоразу підіймаєте цей допис у стрічці, а отже – робите його популярнішим. Якщо ви не погоджуєтеся з автором, краще зробіть на цю тему допис на власній сторінці (можна згадати чи навіть «тегнути» автора поста, який наштовхнув на роздуми). Так ви, по-перше, не допомагатимете просуванню опонента, а по-друге, зробите власну сторінку більш яскравою і відвідуваною.

Не перетворюйтеся на «пластик»

Деякі профілі у Facebook схожі на щоденники «ідеальних людей», які виставляють лише найбільш вдалі фото, завжди скрізь встигають, їм усе вдається. Я такі профілі називаю «пластиковими», бо за ними неможливо роздивитися справжню людину. Звісно, я не закликаю лише скаржитися на життя в соцмережах, але в «успішний успіх», без падінь і провалів, мало хто вірить. Набагато цікавіше слідкувати за людиною, яка поступово йде до своєї мети, іронізує над собою, пише про свої «факапи», щоб інші могли їх уникнути, щиро ділиться радістю невеличких перемог. Така людина викликає емпатію, бо інші користувачі асоціюють її з собою.

Також я не раджу жорстко розмежовувати «себе-людину» і «себе-професіонала». Адже якою якісною не були б товар чи послуга, яку ви пропонуєте, ви як особистість все ж важливіші.

(вгору)

Додаток 9

4.04.2018

Профили россиян в соцсетях «Одноклассники» и «ВКонтакте» сдали кредиторам

Национальное бюро кредитных историй РФ (НБКИ), продолжит поддерживать сервис, проверяющий в социальных сетях личные странички пользователей-заемщиков (InternetUA).

Корпорация Mail.Ru Group, которая владеет сайтами «Одноклассники» и «ВКонтакте», обеспечит техническую поддержку проекту.

Теперь у одного из самых крупных бюро кредитных историй появилась возможность официального применения данных о людях, пользующихся ресурсами Mail.Ru Group. На их основе оно также может оказывать услуги иным организациям. Как заявил представитель Mail.Ru Group, на рынке существует потребность в прозрачном и легальном поиске данных о пользователях социальной сети «ВКонтакте».

Он отметил, что в новом сервисе бюро искать станут лишь по открытым и актуальным данным. Это отличает его от несанкционированных сервисов от иных компаний, зачастую содержащих старую информацию, в том числе, и ту, что пользователь социальной сети захотел удалить или скрыть. При этом представитель корпорации не пояснил, будет ли у НБКИ возможность использования данных о пользователях прочих сервисов, принадлежащих Mail.Ru Group.

У «ВКонтакте» есть пользовательское соглашение, где в пункте 5.8 утверждается, что администрация социальной сети имеет право на:

• использование данных, которые предоставил пользователь;

• передачу этих данных третьим лицам для того, чтобы соблюсти требования текущего российского законодательства, а также защитить интересы и права самой администрации, пользователей и третьих лиц.

С другой стороны, есть правила, защищающие данные о пользователях. В этом документе пункт 5.1.4 утверждает, что пользователь согласен на то, чтобы партнерам и третьим лицам передавали итоги автоматизированной обработки его данных. И применяли при этом разные модели, оценивающие информацию.

Стоит напомнить, что 9-м апелляционным арбитражным судом был частично удовлетворен иск «ВКонтакте», предъявленный к ООО «Дабл», известной по бренду Double Data. Разработчику программного обеспечения, анализирующего большие объёмы данных, запретили пользоваться в своих целях информацией пользователей отечественной соцсети.

Первоначально «ВКонтакте» подавала иск и к «Дабл», и к НКБИ в январе прошлого года. В социальной сети были недовольны оценкой кредитоспособности пользователей соцсети, основанной на данных из их открытых профилей. Более того, эта информация продавалась банкам.

Из иска следовало, что Национальное бюро кредитных историй предлагает финансовым учреждениям сервисы, основанные на разработанных в «Дабл» технологиях. Они обеспечивают извлечение из базы данных пользователей социальной сети: имена и фамилии, информацию об учёбе и работе, анкеты приятелей, сведения о месте рождения и жительства, фотографии, регулярность посещений странички, типа гаджетов.

Как было отмечено в исковом заявлении, ни пользователи «ВКонтакте», ни сама соцсеть не разрешали извлекать материалы такого рода и пользоваться ими в коммерческих целях. В конце лета владельцем социальной сети и бюро было заключено мировое соглашение. НБКИ обязалось не пользоваться технологиями извлечения данных о пользователях, не получив от компании разрешение.

(вгору)

Додаток 10

4.04.2018

Ультиматум Роскомнадзора: Почему в России хотят заблокировать Telegram и получится ли это сделать

Наступило 4 апреля. В этот день заканчивается срок действия ультиматума, выдвинутого Роскомнадзором к мессенджеру Telegram. Теперь ведомство (поскольку в Telegram не выполнили запрашиваемое) может обратиться в суд по поводу блокировки мессенджера на территории России (InternetUA).

В самом Telegram решения о блокировке особо не опасаются, и на то есть причины. В общем, попробуем разобраться, что, собственно, происходит.

Чего Роскомнадзор хочет от Telegram?

Все дело в «пакете Яровой».

В 2016 году Госдума России приняла пакет законов под авторством депутатов Ирины Яровой и Виктора Озерова.

Среди прочего принятое законодательство обязывало мессенджеры и социальные сети независимо от страны их происхождения выдавать ФСБ секретные криптографические ключи (ключи шифрования).

В противном случае мессенджерам и соцсетям грозили штраф на сумму до 1 млн руб и блокировку.

То есть Роскомнадзор обратился к Telegram с требованием «Отдай ключи!»

Как все происходило

Для начала, чтобы потребовать у Telegram ключ, мессенджер надо было внести в Реестр распространителей информации.

Для того чтобы внести мессенджер в реестр, сначала надо было получить у него его контактные данные.

Создатель Telegram Павел Дуров требование предоставить контактные данные сперва игнорировал. Потом сказал, что их можно найти в открытых источниках, а против внесения в реестр он не возражает.

Следующий раунд противостояния произошел 26 июня 2017 года. Дуров на своей странице в «ВКонтакте» сообщил следующее:

«Глава Роскомнадзора заявил, что Telegram должен выдать спецслужбам “ключи для дешифрации”, чтобы те могли читать переписку пользователей и ловить террористов. Это требование не только противоречит 23-й статье

Конституции РФ о праве на тайну переписки, но и демонстрирует незнание того, как шифруется коммуникация в 2017 году».

Он уточнил, что «в 2017 году обмен секретной информацией построен на окончательном шифровании, к которому у владельцев мессенджеров нет и не может быть “ключей для дешифрации”», а хранятся подобные ключи на устройствах самих пользователей.

Ну, и в качестве резюме Дуров написал, что потенциальная блокировка Telegram «никак не усложнит задачи террористов и наркодилеров» из-за наличия других мессенджеров, работающих по принципу окончательного шифрования.

«Чтобы победить терроризм через блокировки, придется заблокировать интернет», – добавил он.

Далее было 12 июля 2017 года и запрос ФСБ в лондонский офис Telegram касательно информации о переписке шести пользователей мессенджера.

Через несколько месяцев, в конце сентября, Дуров опубликовал извещение ФСБ о составлении в его отношении протокола об административном нарушении за невыполнение требования.

Последний (на данный момент) акт этого противостояния вынесем, пожалуй, отдельно. У него даже есть свое название.

Ультиматум

Верховный суд России 20 марта признал законным требование ФСБ предоставить ключи шифрования Telegram.

Далее был ультиматум: Роскомнадзор дал Telegram 15 дней на передачу ключей для расшифровки переписок ФСБ. Этот срок истекает 4 апреля.

В то же время был подан коллективный иск 35 пользователей мессенджера, считавших требование о предоставлении ключей для расшифровки переписок незаконным. Однако 23 марта Мещанский суд Москвы этот иск отклонил.

Позиция Telegram

Частично о ней сказано выше. В мессенджере подчеркнули, что не предоставят ключи, просто потому что технически не могут это сделать.

Представитель Telegram в судах Павел Чиков 2 апреля опубликовал скриншот письма, отправленного юристами мессенджера в Роскомнадзор в ответ на требование ФСБ.

В нем говорится, что у мессенджера нет технической возможности предоставить спецслужбам необходимые им данные.

В Роскомнадзоре заявили, что официального ответа от Telegram не получили.

Получится ли заблокировать Telegram?

Вряд ли. По крайней мере в этом уверено большинство специалистов.

«Скорее всего, у нас будет что-то вроде иранского сценария. В Иране государство тоже блокирует доступ к Telegram, пытается это делать, но подобные блокировки пользователи Telegram обходят с помощью таких технологий, как VPN и прокси… Пользователи могут установить VPN – сейчас

это сделать можно без каких-то специальных технических навыков. Также команда разработчиков встроила в Telegram функцию, которая позволяет включить прокси одной ссылкой, что существенно упрощает обход блокировок для конечных пользователей, которые не обладают специальными техническими навыками», – цитирует BFM.ru Александра Литреева, руководителя одной из компаний, занимающихся разработкой VPN.

Павел Дуров еще 20 марта на своей странице в Twitter написал, что «угрозы заблокировать Telegram не принесут плодов».

В Российской ассоциации электронных коммуникаций (РАЭК) заявили, что «полная блокировка мессенджера невозможна, в ряде случаев перестанут работать лишь некоторые функции».

Но в Роскомнадзоре, похоже, иного мнения.

(вгору)

Додаток 11

9.04.2018

ФБР арестовало один из старейших в мире сайтов объявлений

ФБР арестовало сайт Backpage.com, который обвиняется в размещение объявлений о сексуальных услугах и рабстве. Соответствующий раздел сайта был закрыт более года назад, но авторы просто перенесли свои объявления в другие разделы. Арест был произведен на фоне принятия в США закона, по которому операторы онлайн-площадок начнут нести ответственность за содержание материалов, размещенных третьими лицами (InternetUA).

Арест Backpage.com

Правительство США арестовало Backpage.com – один из самых старейших и известнейших в интернете сайтов объявлений, основанный в 2004 г. При входе на главную страницу сайта посетитель видит сообщение об аресте. Причиной стало то, что на сайте размещались объявления, касающиеся проституции и сексуального рабства.

Арест был осуществлен силами Федерального бюро расследований (ФБР), Инспекции почтового обслуживания США, Налогового управления США, Объединенного разведывательного центра и других ведомств.

Юридическая база

Напомним, в середине марта Сенат – верхняя палата Конгресса, американского парламента – одобрил законопроект о ликвидации возможностей для секс-торговли в интернете (Stop Enabling Sex Traffickers Act, SESTA). Секс-торговля включает в себя сексуальное рабство и коммерческую сексуальную эксплуатацию человека. Новый закон вводит криминальную ответственность для сайтов, распространяющих объявления и рекламу в этой сфере. Месяцем ранее Палата представителей – нижняя палата Конгресса – одобрила свою редакцию этого закона, позволяющую штатам и жертвам бороться с секс-торговлей онлайн (Allow States and Victims to Fight Online Sex Trafficking Act, FOSTA).

Юридически пакет FOSTA-SESTA представляет собой набор поправок к закону «О приличиях в области связи», принятому в 1996 г. Так называемая Секция 230 этого закона гарантировала, что провайдеры и операторы интернет-платформ не несут ответственности за содержание материалов, которые размещают на платформах третьи лица.

Раскол ИТ-отрасли

Интернет-активисты и представители ряда технологических компаний подвергли пакет FOSTA-SESTA критике, поскольку фильтрация контента и удаление материалов, касающихся секс-торговли, может стать трудновыполнимой обязанностью для небольших компаний. Фонд электронных рубежей недоволен законом, так как он фактически легализует цензуру со стороны онлайн-платформ по отношению к пользователям.

Пакет FOSTA-SESTA расколол американские технологические компании на два лагеря, отмечает ресурс The Verge. Например, Oracle и IBM горячо поддерживают новые меры, а Google и Facebook по большей части хранят молчание, хотя именно их новый закон затронет в первую очередь. С другой стороны, некоммерческая организация «Фонд Викимедиа» заявила, что проекты типа Википедии вообще не смогут существовать без гарантий, предоставляемых Секцией 230.

Криминальная история Backpage.com

Backpage.com был создан в 2004 г. компанией New Times Media, позднее переименованной в Village Voice Media. К 2011 г. площадка стала вторым по величине сайтом объявлений в США — она уступала только проекту Craigslist. До января 2017 г. на Backpage.com существовал раздел для взрослых, где размещались объявления об услугах и вакансиях в секс-индустрии, в том числе в области эскорта, эротического массажа, стриптиза, телефонного секса и т. д. После того, как в 2010 г. Craigslist закрыл собственную рубрику аналогичного содержания, раздел для взрослых на Backpage.com приобрел огромную популярность.

В 2015 г. власти США заподозрили сайт в причастности к сексуальному рабству и сексуальной эксплуатации несовершеннолетних. В частности, американский Национальный центр пропавших без вести и эксплуатируемых детей утверждал, что через Backpage.com была осуществлена продажа в рабство 420 несовершеннолетних. Началось расследование, в ходе которого в октябре 2016 г. был арестован гендиректор компании Карл Феррер (Carl Ferrer), однако позднее и он, и основатели проекта были оправданы как раз на основании Секции 230.

В итоге Backpage.com приостановил работу раздела для взрослых, обвинив власти в незаконной цензуре. Однако многие авторы объявлений об эскорт-услугах и эротическом массаже просто перенесли свои материалы в рубрики «Массаж» и «Женщины ищут мужчин». Напомним, в США запрещена проституция, за исключением нескольких регионов в штате Невада.

(вгору)

Додаток 12

28.03.2018

Вредоносы для Android скрывались под видом полезных утилит

SophosLabs предупредила о новых вредоносных программах, найденных в магазине Google Play, которые прятались под видом полезных утилит. Эксперты идентифицировали это семейство вредоносных программ как Andr/HiddnAd-AJ. Они заполняют зараженное устройство рекламой, но только после того, как прошло время после установки, чтобы усыпить бдительность пользователей. Компания сообщила о находках в Google, и приложения уже удалены из Play Store, но некоторые из них получили достаточно большую популярность, а суммарное количество загрузок превысило 500000 (Компьютерное Обозрение).

Уловки, используемые разработчиками для того, чтобы пройти процесс проверки приложений Play Protect, оказались на удивление простыми. Во-первых, приложения имели, по крайней мере на поверхности, заявленную в описании функциональность: шесть из них были приложениями для сканирования QR-кодов, а еще одно – так называемым «умным компасом». Во-вторых, мошенники не сразу запускали вредоносную часть своих приложений, скрываясь в течение нескольких часов, прежде чем развязать «рекламную кампанию».

В-третьих, рекламная функциональность каждого приложения была встроена в часть кода, которая выглядела на первый взгляд, как стандартная библиотека для Android. Добавив «графический» компонент в коллекцию подпрограмм, которые обычно находятся в приложениях для Android, механизм рекламного ПО внутри приложения эффективно скрывался практичести на поверхности.

При всей своей невысокой опасности, эта вредоносная программа, однако, не только показывает всплывающие рекламные объявления, но также может отправлять уведомления от лица Android, в том числе размещать в них интерактивные ссылки, чтобы повысить доход от рекламы для злоумышленников.

(вгору)

Додаток 13

28.03.2018

Ольга Карпенко

Mozilla выпустила дополнение для Firefox, блокирующее «слежку» Facebook за пользователем

Компания Mozilla, разработчик популярного браузера Firefox, создала специальное дополнение для него, которое блокирует трекинг действий пользователя со стороны социальной сети Facebook. Дополнение бесплатно и называется Facebook Container (AIN.UA).

Как объясняют в компании, Facebook Container после установки изолирует все личные данные пользователя Facebook в отдельный контейтер, что затрудняет для сети отслеживание визитов пользователя на другие сайты, cookies на этих сайтах и т.д. Установка этого дополнения удаляет все cookies Facebook и вылогинивает пользователя из сети.

Если пользователь опять залогинится в сеть, она запустится в отдельной вкладке бразуера, помеченной голубым цветом. При переходе на другой сайт пользователь «выйдет» из контейнера и сможет браузить интернет как обычно. Но если он, к примеру, нажмет на кнопку «Поделиться», он опять вернется в этот режим.

«Вы должны знать, что использование подобных кнопок передает информацию Facebook о том, с какого сайта вы перепостили информацию», – предупреждают в компании.

При активном дополнении не будут работать встроенные комментарии Facebook, счетчики лайков и другие функции сети на внешних сайтах. Это не даст сети собирать данные об активности пользователя на этих сайтах. Также, могут быть проблемы с сайтами, где пользователь авторизируется с помощью своего Facebook-аккаунта.

Дополнение никак не может повлиять на то, какие данные уже есть у Facebook или же какие данные о пользователе компания разрешила получать третьим сторонам. Сеть все еще будет иметь доступ ко всему, что вы делаете на сайте сети, включая комментарии, загрузки фото, лайки, все данные, которыми вы делитесь с Facebook-приложениями.

(вгору)

Додаток 14

28.03.2018

Хакерская группировка Cobalt продолжает атаковать банки

Исследователи безопасности из компании Group-IB зафиксировали новую кибератаку хакерской группировки Cobalt, также известной как Carbanak и Anunak. Хакеры продолжают проявлять активность даже после ареста человека, предположительно являющегося лидером группировки (InternetUA).

По словам экспертов, злоумышленники осуществили очередную фишинговую рассылку, на этот раз от имени компании SpamHaus, специализирующейся на защите от спама и фишинга. В отправленных с поддельного адреса j.stivens@spamhuas[.]com письмах утверждалось, что IP-адреса жертв были заблокированы из-за подозрений в рассылке спама. Далее получателям предлагалось перейти по ссылке, ведущей на страницу загрузки документа Microsoft Office, содержащего вредоносное вложение.

Изучив структуру атаки, специалисты отдела анализа вредоносного кода подтвердили, что за рассылкой стоит именно Cobalt.

«Мы не исключаем, что оставшиеся на свободе члены Cobalt некоторое время будут продолжать атаки, в том числе, чтобы показать, что их

задержанные подельники не причастны к этой группе. Однако, учитывая арест лидера группы, такие атаки вскоре сойдут на нет. Вероятнее всего члены Cobalt примкнут к действующим группам или, в результате, очередного „передела“ появится новая киберкриминальная структура, атакующая банки в разных странах. В любом случае, не стоит списывать со счетов наследие Cobalt – и с точки зрения ресурсов, и с точки зрения инструментария», – заявил руководитель департамента Threat Intelligence и CTO Group-IB Дмитрий Волков.

Хакерская группировка Carbanak активна как минимум с 2013 года. С помощью вредоносного ПО Anunak киберпреступники атаковали электронные платежные системы и банки в 40 странах по всему миру. В 2016 году киберпреступники переключились с Anunak на более сложное ПО Carbanak, использовавшееся до 2016 года, а затем вооружились еще более усовершенствованным инструментом, созданным на основе программы для проведения тестов на проникновение Cobalt Strike. С помощью вредоносного ПО злоумышленники заставляли банкоматы выдавать наличные.

(вгору)

Додаток 15

29.03.2018

Уязвимость сети: как защитить свои данные в интернете

Данные 50 млн человек попали в чужие руки. Эксперты: нужно настроить соцсети и пользоваться VPN

В мире не утихает скандал вокруг утечки информации из популярной соцсети Facebook. Выяснилось, что частная компания по анализу данных собрала на просторах сети личную информацию около 50 млн пользователей и использовала ее без разрешения для влияния на американские выборы. В результате за неделю акции Facebook упали на $58 млрд, а возмущенные пользователи запустили флешмоб под хештегом #deletefacebook, призывая удалять свои аккаунты из соцсети. Бойкот поддержали многие IT-инвесторы, известные актеры, Илон Маск (InternetUA).

Глава Facebook Марк Цукерберг в ответ на шумиху пообещал сделать сервис безопаснее, ввести проверку приложений «с подозрительной деятельностью» и уменьшить объем запрашиваемой у пользователей информации.

Но история уже заставила пользователей задуматься о цифровой гигиене во всемирной паутине. «Сегодня» пообщалась с экспертами и выяснила, что делать украинцам, чтобы защитить свои персональные данные на просторах интернета.

В сети: без куки и истории

По мнению IT-специалиста Вячеслава Троицкого, во всемирной сети интернет контролировать доступ к своим данным проще, чем в соцсетях.

«Если в Facebook делятся своим контентом с друзьями, то на сторонних сайтах мало кто станет просто так сливать свои данные», – отмечает эксперт.

Однако и здесь, по его мнению, необходимо соблюдать некоторую осторожность. Троицкий рекомендует не пользоваться публичными беспроводными сетями, поскольку через них данные воруют чаще всего.

«Если же подключение все равно необходимо, лучше выходить через VPN-приложения, которые обеспечивают шифрованное соединение (анонимность в сети)», – рассказал нам специалист.

Сохранить личные данные в закрытом доступе поможет и отключение cookie (куки) – небольших файлов, которые собирают для сайтов информацию о посещаемых веб-страницах. В большинстве браузеров куки отключаются в настройках во вкладке «Настройки контента». При этом есть и другой способ не оставлять цифровой след – выходить в интернет через режим «Инкогнито», который не сохраняет историю просмотров и информацию, вписанную на сайтах. Стоит также игнорировать баннеры и всплывающие окна на сайтах и подозрительные ссылки в письмах на е-почту.

В соцсетях: покопаться в настройках

«Лучший способ запретить соцсетям собирать о вас информацию – перестать ими пользоваться», – говорит эксперт по информационной безопасности Игорь Шиляк. Тем же, кто не может совсем отказаться от соцсетей, специалист советует ответственно отнестись к их настройке:

«В случае с Facebook нужно запретить сторонним компаниям собирать ваши данные. Для этого нужно зайти на страницу “Приложения”, в этом разделе нажать кнопку “Редактировать”, а после – Disable platform (англ. – отключить платформу)».

По словам Шиляка, это отключит приложения вовсе. Менее радикальный шаг – на странице «Приложения» снять отметки со всех категорий данных, которые вы им предоставляете (семейное положение, дата рождения). Эксперт настаивает и на фильтрации того, что попадает в соцсеть.

«Фотографии, лайки, переходы со страницы и даже список друзей многое говорят о человеке и его предпочтениях. Эти данные позволяют компаниям подсовывать народу подходящую рекламу и манипулировать их мнением», – поясняет Шиляк.

Чтобы максимально обезопасить свою информацию, нужно публиковать в соцсетях самый минимум, не переходить по рекламным ссылкам и не проходить развлекательные тесты – они тоже собирают информацию о пользователях.

«Нельзя писать в переписках данные паспорта, прописки, банковских карт, пароли и логины. Нет гарантий, что этими данными не воспользуются злоумышленники, взламывающие аккаунты», – говорит эксперт и добавляет, что необходимо создать сложные пароли минимум из 8 знаков. В идеале – из прописных и заглавных букв, цифр и символов.

Шопинг: протокол и доверие

Особенно осторожно нужно отнестись к покупкам онлайн. Ведь интернет-магазины запрашивают такие данные, как имя/фамилия, номер телефона (для обратной связи), место проживания (для доставки) и номер банковской карты (для оплаты товара).

Чтобы эту информацию не использовали злоумышленники, в первую очередь нужно выбирать только проверенные торговые интернет-площадки, а перед покупкой тщательно изучать отзывы о магазине.

«Важно, чтобы магазин использовал для оплаты только международные системы безопасности, сертифицированные компаниями Visa и MasterCard», – рассказал Игорь Шиляк.

Он добавил, что об этом свидетельствуют соответствующие логотипы компаний на странице, а также зеленый индикатор защищенного протокола HTTPS в адресной строке. Но, чтобы удостовериться наверняка, лучше позвонить в онлайн-магазин и спросить у сотрудников, как обеспечивается безопасность персональных данных. К этому вопросу компания должна относиться максимально серьезно. Если работникам магазина ничего не известно о защите личной информации, лучше воздержаться от покупок на этом сайте.

«Также рекомендуется для покупок в интернете завести отдельную банковскую карту и пополнять ее непосредственно перед шопингом», – говорит эксперт.

По его мнению, то же касается и электронной почты – лучше завести отдельный адрес, куда и будут приходить подтверждающие письма от магазинов, а также их рассылка. Не стоит забывать и об опасности публичного wi-fi. Преступники могут перехватить незашифрованные данные банковских карт и воспользоваться ими. Потому покупки стоит отложить до того момента, пока рядом не окажется защищенное соединение.

(вгору)

Додаток 16

2.04.2018

Acronis: более 40 % пользователей никогда не слышали о вредоносах-вымогателях

Ежегодно Acronis проводит глобальный опрос потребителей, который приурочен к Всемирному дню резервного копирования (World Backup Day), который отмечается 31 марта, чтобы оценить отношение, привычки и знания общественности касательно защиты данных. В этом году компания опросила интернет-пользователей из США, Великобритании, Австралии, Германии, Испании, Франции и Японии (Компьютерное Обозрение).

Как оказалось, в этом году по сравнению с прошлогодним опросом, больше респондентов были проинформированы об онлайновых угрозах, связанных с вымогательством, но при этом уменьшилось число людей,

использующих резервное копирование, и больше опрошенных сообщили о потере данных.

В обзоре были рассмотрены две области: общие темы резервного копирования и конкретные вопросы об осведомленности о вымогательстве.

Общие выводы о резервном копировании показали:

•31,4 % признали, что не создают резервные копии своих личных данных;

•35,7 % респондентов сказали, что они или члены их семьи потеряли данныеж;

•47,2 % сообщили, что когда они делают резервное копирование, они используют облако в качестве места для хранения копий.

Что касается вымогательства данных:

•41,8 % респондентов заявили, что никогда не слышали о вредоносах-вымогателях – и хотя это все еще огромное число, но показатель прошлого года улучшился более чем на 20 %;

•56 % опрошенных понимают, что ransomware может захватить систему и уничтожить файлы;

•только 6,9 % готовы платить более 140 долл. за восстановление потерянных данных.

Что касается перспектив, то Acronis прогнозирует, что в результате роста числа вымогателей, более изощренных методов атак и недостаточной осведомленности пользователей, 2018 г. станет самым тяжелым годом в области кибератак и случаев потери данных.

(вгору)

Додаток 17

3.04.2018

Хакер зламував сторінки у соцмережах і вимагав гроші за відновлення

За допомогою фішингу киянин відбирав у власників доступ до їх персональних сторінок, після чого вимагав за нього гроші. Такі дії зловмисника кваліфіковані поліцією за двома статтями Кримінального кодексу України (InternetUA).

Працівники Київського управління Департаменту кіберполіції Нацполіції та слідчі Голосіївського управління поліції Києва, за процесуального керівництва Київської міської прокуратури №1, встановили 23-річного хакера.

Крім персональних сторінок, він також орієнтувався на профілі Інтернет-магазинів у соціальній мережі «Instagram». Використовуючи фейкові сторінки та електронні листи, нібито від адміністрації «Instagram», зловмисник отримував доступ до зазначених сторінок. Після чого надсилав потерпілим Email-повідомлення, в яких пропонував за 10 тисяч гривень розблокування сторінки.

Оперативники з кіберполіції провели санкціонований обшук за місцем проживання хакера. У його помешканні виявлено комп’ютерну техніку та

мобільні телефони з різними сім картками, які зловмисник використовував для реєстрації фейкових доменних імен. Також, у квартирі вилучено блокнот з чорновими записами, де зловмисник записував усі операції по руху коштів.

Триває досудове розслідування за двома статтями Кримінально кодексу України: за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ч. 3 ст. 190 (Шахрайство) КК України.

Поліцейські встановлюють осіб, які стали жертвами дій зловмисника. Вилучену комп'ютерну техніку направлено до експертного центру для проведення усіх необхідних експертиз. Після отримання її результатів буде вирішено питання щодо оголошення киянину про підозру.

(вгору)

Додаток 18

3.04.2018

Михаил Сапитон

Google Chrome сканирует пользовательские файлы на Windows. Это не опасно

Браузер Google Chrome, рыночная доля которого перевалила за 60 %, подвергся нападкам ряда пользователей Twitter. Они обнаружили, что браузер сканирует их компьютеры на Windows. Проверке подвергаются, в том числе, и документы из пользовательских папок, не связанных с системными функциями или установкой софта. На ситуацию обратило внимание издание Motherboard (AIN.UA).

Оказалось, что подозрительная активность Chrome – результат работы новой антивирусной функции, созданной в партнерстве с компанией ESET. Опция называется Chrome Cleanup Tool и сканирует содержимое компьютера на предмет вредоносного софта, который может спровоцировать изменения в работе самого Chrome. Если в ходе мониторинга такие угрозы будут обнаружены, метаданные файла, в котором записана малварь, отправляются в Google. Следом программа просит у пользователя разрешения удалить подозрительные документы. Отправку сведений в Google можно отменить, убрав галочку подтверждения с поля Report details to Google в настройках Chrome.

Обновление Chrome Cleanup Tool представили еще в октябре 2017 года. В компании заверили, что инструмент не способен, например, увидеть пользовательские фотографии или прочитать документы – его единственной целью является отслеживания и удаление вредоносных дополнений. Они могут спровоцировать утечку данных или появление рекламы в нежелательных местах. Келли Шортбридж, которая начала дискуссию о работе Chrome в Twitter, уточнила свои претензии в комментарии Motherboard:

В нынешней ситуации, меня действительно шокирует, что Google так тихо выкатили эту функцию, не опубликовав больше сопроводительной

документации – хотя бы чтобы избежать спекуляций. Их намерения очевидно сфокусированы в области безопасности, но отсутствие явного согласия и прозрачности нарушает их собственные критерии «дружественного к пользователям софта», о которых сообщают правила Chrome Cleanup Tool.

Реакция Шортбирдж спровоцировала много внимания и повлекла ответ главы отдела безопасности Google Chrome Джастина Шу. Он уточнил, что инструмент запускает раз в неделю, имеет права обычного пользователя и работает в закрытой «песочнице» (то есть код Cleanup Tool изолирован от других программ). Наконец, Шу считает что требование подтвердить удаление файлов – достаточное проявление прозрачности со стороны Google.

Для сравнения, некоторые антивирусные решения сканируют всю систему, пользуясь правами администратора, и регулярно загружают данные на сервера компании. Тем не менее, как отмечает Motherboard, многие пользователи оказались просто напуганы тем, что браузер, оказывается, регулярно прочесывает их компьютер в поисках вредоносных файлов.

(вгору)

Додаток 19

4.04.2018

Игра для Android скрытно подписывала пользователей на платный сервис

Специалисты ESET обнаружили новую мошенническую схему. Приложение Pingu Cleans Up подписывало пользователей на дорогостоящий сервис, используя легитимный способ оплаты в Google Play (Компьютерное Обозрение).

Игра Pingu Cleans Up впервые появилась в магазине приложений 8 февраля. Ее загрузили от 50 до 100 тыс. раз.

После установки на планшет или смартфон приложение предлагало создать игрового персонажа. На первых двух этапах потенциальная жертва, выбирая нужный атрибут, должна была нажать кнопку «Подтвердить» во всплывающем окне.

На последнем этапе пользователь с банковской картой, привязанной к аккаунту Google Play, видел окно, напоминающее предыдущие. Разница в том, что кнопка «Подтвердить» была заменена на «Подписаться». Нажав на кнопку, пользователь оформлял подписку стоимостью 5,49 евро в неделю. Платеж списывался с карты автоматически до момента отмены подписки.

Пользователи, в аккаунте которых не было данных банковской карты, видели на третьем этапе другое окно. Им предлагалось добавить информацию о способе оплаты, чтобы завершить покупку.

Схема мошенников основана на предположении о том, что некоторые пользователи кликнут по любому окну, мешающему игре, не вчитываясь в текст. Судя по негативным отзывам в Google Play, афера работает.

После предупреждения ESET игра Pingu Cleans Up была удалена из Google Play. Пострадавшим не нужно отключать подписку вручную – она отменена автоматически.

ESET рекомендует изучать рейтинг и отзывы в Google Play до установки приложения и использовать мобильный антивирус для смартфонов и планшетов на Android.

(вгору)

Додаток 20

4.04.2018

Google исправила более 300 уязвимостей в ОС Android

Компания Google выпустила обновление для операционной системы Android, исправляющее в общей сложности 312 уязвимостей, из которых 9 являются критическими и позволяют злоумышленнику удаленно выполнить произвольный код. При этом 287 проблемам была присвоена высокая степень опасности (InternetUA).

В компоненте Android runtime была исправлена 1 уязвимость (CVE-2017-13274), позволяющая злоумышленнику добиться повышения привилегий на системе.

Также была исправлена 1 проблема (CVE-2017-13275) во фреймворке, позволяющая вредоносным приложениям обходить защитные решения операционной системы, изолирующие данные приложений друг от друга.

В медиа-фреймворке были исправлены 5 уязвимостей (CVE-2017-13276 - CVE-2017-13280), в том числе 2 критические (CVE-2017-13276, CVE-2017-13277). Уязвимости позволяли удаленному злоумышленнику использовать специально сформированный файл для выполнения произвольного кода в контексте привилегированного процесса, а также повысить привилегии на системе и добиться отказа в обслуживании.

Кроме того, было исправлено 12 проблем в системе, в том числе 5 критических (CVE-2017-13281 - CVE-2017-13283, CVE-2017-13267, CVE-2017-13285). Уязвимости позволяли злоумышленнику повысить привилегии, удаленно выполнить произвольный код и добиться отказа в обслуживании.

В компонентах Broadcom была исправлена 1 критическая уязвимость (CVE-2017-13292) в драйвере bcmdhd.

3 уязвимости (CVE-2017-13293, CVE-2017-5754, CVE-2017-1653) были исправлены в компонентах ядра. Наиболее серьезная уязвимость позволяла локальному вредоносному приложению выполнять произвольный код в контексте привилегированного процесса.

Наибольшее количество уязвимостей было исправлено в различных компонентах Qualcomm. В общей сложности было исправлено 289 уязвимостей разной степени опасности. Из них 8 являлись критическими (по классификации производителя).

(вгору)

Соціальні мережі
як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

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.