СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(4.09–18.09)

2018 № 16

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(4.09–18.09)
№ 16

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

3.09.2018
Microsoft проведет работу над ошибками и вернет прежний Skype

Около года назад Microsoft представила новое приложение Skype с полностью измененным дизайном и функцией Highlights. Это аналог историй из Instagram и Snapchat. В погоне за популярностью разработчики сервиса попытались украсть особенности конкурентов, чтобы сделать свой продукт «лучше». На деле вышло не очень хорошо. Да и тем, кто использует Skype на постоянной основе, новая функция пришлась не по вкусу (Portaltele).

Но сотрудники Microsoft признали ошибку и скоро ее исправят. Чтобы сделать Skype «проще и привычнее», разработчики сервиса удалят из него Highlights 30 сентября 2018 года.

«В прошлом году мы экспериментировали с одним из наших продуктов и добавили несколько новых функций. Но наши пользователи сказали, что мы переборщили, сделав Skype слишком сложным. Большинству эти изменения не понравились, и мы решили сделать шаг назад. Мы хотим снова сделать Skype удобным», – сообщили сотрудники компании.

Помимо исчезновения Highlights, пользователей порадуют упрощенной навигацией по интерфейсу. А в Skype для компьютеров появится старая тема оформления для тех, кто так и не смог привыкнуть к новому стилю приложения.

***

4.09.2018
Пользователи сообщили о сбое в работе Facebook

Пользователи Facebook сообщили о сбоях в работе социальной сети. Об этом свидетельствуют данные портала Downdetector.com, который отслеживает перебои в работе онлайн-сервисов (InternetUA).

Пользователи рассказали, что не могут зайти в свои аккаунты в соцсети. Также некоторые пожаловались на недоступность мессенджера и Instagram, который также принадлежит Facebook.

По данным портала, жалобы на перебои в работе поступили из Японии, Казахстана, Финляндии, Украины, Польши, Германии, Италии, Франции, Португалии, Великобритании, а также из США, Канады и некоторых стран Африки и Южной Америки.

***

4.09.2018
Twitter начнет показывать, кто сейчас в сети

С момента основания в Twitter никогда не отображался статус онлайн, но в скором времени это изменится (InternetUA).

Череда противоречивых изменений в Twitter, кажется, не закончится уже никогда. В этот раз создатели соцсети решили переосмыслить систему ответов на твиты, превратив их в мини-чаты, похожие на таковые в iMessage и WhatsApp.

Также в этих окнах будет отображаться статус пользователей. Это значит, что теперь каждый участник разговора узнает, кто из собеседников сейчас в сети.

Подобный дизайн интерфейса значительно ускорит общение в соцсети, а также выделит твиты того, кто начал общение (фиолетовые и синие сообщения).

О нововведениях сообщила одна из сотрудниц соцсети Сара Хайдер. А затем об этом упомянул основатель сервиса @jack.

Пользователи, ознакомившиеся с потенциальными изменениями, в большинстве своем отреагировали негативно. Они отметили, что аудитория Twitter любит его именно за схожесть с классическими блогами и простоту.

***

4.09.2018

WhatsApp лишился поддержки iPhone 4 и стал безопаснее

Разработчики WhatsApp представили обновленную версию фирменного мессенджера для платформы iOS, которая уже доступна для загрузки в App Store.

Докладніше

***

5.09.2018

Звонки в Skype теперь можно записывать

4 сентября Microsoft объявила, что добавила функцию записи звонков в последнюю версию Skype для macOS и iOS.

Разработчики Skype заявляют, что новая функция записи звонков является облачной, а приложение информирует каждого участника беседы о том, что идёт запись.Запись видеочатов включает в себя изображения с экранов всех задействованных пользователей и её можно сохранить или переслать в течение 30 дней. Вариант записи только аудио отсутствует. Как в мобильной, так и в Mac-версии запись вызова может быть инициирована нажатием на значок «+» в нижней части экрана и выбором опции «Начать запись». После начала записи звонка, участники получат уведомление (PortalTele).

Новая функция доступна в обновлённой версии Skype, которую можно загрузить с веб-сайта Skype или в App Store.

***

6.09.2018

Йдемо. Понад чверть американців запевняють, що відмовилися від додатку Facebook // Користувачі кажуть, що залишають Facebook

Понад чверть користувачів Facebook із США кажуть, що вони видалили додаток соцмережі зі своїх телефонів за останній рік. Це відбувається як свого роду реакція на проблеми соцмережі із забезпеченням конфіденційності користувачів.

Докладніше

***

11.09.2018

Instagram разрешит отмечать друзей на видео

Принадлежащий Facebook сервис Instagram вскоре получит новую функцию, позволяющую отмечать друзей на видео. Команда сервиса уже тестирует её (IGate).

В отличие от фотографий, где пометки показываются поверх изображения, в видео потребуется нажать на специальную кнопку и тогда все отмеченные пользователи будут показаны списком на отдельной странице.

На данный момент такие ролики не появляются в профиле отмеченного пользователя, как это происходит с фотографиями. Однако это может измениться к моменту широкого запуска для всех пользователей Instagram.

На данный момент функция доступна ограниченному числу пользователей и работает только в мобильном приложении, а в веб-интерфейсе недоступна.

***

11.09.2018

Топ 10 найпопулярніших сайтів серед українців

Російська соціальна мережа «ВКонтакте» за підсумками серпня залишилася на четвертому місці по відвідуваності в Україні. Це не може не дивувати, так як на цей сайт без зміни ip-адреси неможливо зайти. За даними дослідження Factum Group Ukraine, російські «Яндекс» і «Одноклассники» також знаходяться в першій десятці по відвідуваності, хоча і вони вже давно заблоковані провайдерами на території країни (znaj.ua).

На першому місці за відвідуваністю в Україні знаходяться Google, YouTube, Facebook. Тут все зрозуміло і очевидно, оскільки ця трійця залишається незмінною. Так, середньоденна частка аудиторії за місяць для доменів Google незначно скоротилася і склала 64 % а місячний охоплення аудиторії – 83 %. Для Youtube ці показники становлять 42 % і 69 %, для Facebook – 32% і 54%.

Середньоденний і місячний охоплення української аудиторії для «ВКонтакте» склали 16 % і 32 % відповідно. У десятку найпопулярніших ресурсів також увійшли сайти OLX, «Приватбанк», «Яндекс», «Одноклассники» і Instagram, що змістив з 10 на 11 місце сервіс прогнозу погоди «Синоптик»". Особливих змін немає. Варто відзначити, що це досить несподівана статистика. Нагадаємо, що російські сайти вже протягом кілька років перебувають під забороною, і провайдери закрили доступ до цих сервісів.

***

12.09.2018
Мессенджер WhatsApp теперь доступен для кнопочных телефонов

На странице официального блога WhatsApp сообщается, что мессенджер стал доступен для кнопочных телефонов. Правда пока не для всех, а только для аппаратов JioPhone популярных в Индии. Разработчики создали специальную оптимизированную версию приложения, работающую на операционной системе KaiOS (DroidBug).

Сообщается, что для мессенджера WhatsApp на JioPhone доступны все основные функции, включая обмен сообщениями, изображениями, видео, запись и отправка голосовых сообщений, как в личных, так и в групповых чатах. Также для всех сообщений работает сквозное шифрование.

Оптимизированное приложение WhatsApp доступно для телефонов JioPhone в фирменном онлайн-магазине приложений.

***

12.09.2018
Skype научился отправлять SMS с ПК
Ян Глинка

Microsoft начала тестирование сервиса SMS Connect для Android-приложения Skype. Сервис компании позволяет с помощью настольного компьютера отправлять и получать SMS. Skype SMS Skype SMS Пока новая функция доступна только для тестировщиков программы Skype Insiders, однако с течением времени она должна появиться и в обычной версии приложения. С помощью SMS Connect с Android-смартфона можно подключить ПК на базе Windows/macOS. Благодаря этому с компьютера можно не только продолжать SMS-переписку, но и начинать новые диалоги и получать фото – и видеофайлы в виде MMS. Для подключения сервиса нужно зайти на свою учетную запись в Android-приложении и выбрать в настройках пункт «Включить SMS Connect». Подсказки на экране покажут дальнейшие действия (Bad Android).

***

12.09.2018
Проявлять эмоции в Instagram стало проще и быстрее

Очевидно, что в современном мире, когда мы все больше общаемся с коллегами, друзьями и близким при помощи мессенджеров и социальных сетей, всевозможные виды смайликов или эмодзи стали неотъемлемой частью нашей жизни (InternetUA).

Компания Instagram постоянно работает над улучшением функционального списка возможностей своей соцсети. В течение последних нескольких месяцев компания работала над новой функцией, которая стала доступна пользователям смартфонов несколько дней назад.

Речь идет о панели с наиболее часто используемыми вами смайликами, которая располагается над виртуальной клавиатурой. После обновления приложения до последней версии вы сможете быстро выбирать любимые эмодзи, не переключая клавиатурную раскладку. Это повышает удобство при использовании и увеличивает скорость набора.

Обновление стало доступно одновременно на двух мобильных платформах iOS и Android.

***

12.09.2018 126

В мобильном приложении YouTube появилась новая функция // YouTube добавил счетчик времени просмотренных видео

На конференции разработчиков Google I/O 2018 компания анонсировала появление ряда инструментов, направленных на то, чтобы пользователи сервисов лучше понимали, на что конкретно они тратят время.

Докладніше

***

12.09.2018

Розроблений у Facebook штучний інтелект Rosetta допоможе соцмережі зрозуміти меми

Найбільша соцмережа планети Facebook адаптувала свою систему штучного інтелекту Rosetta, яка вже займається перекладами та пошуком хейтерських фраз, для розпізнавання тексту на зображенні.

Докладніше

***

13.09.2018

В Pinterest уже более 250 млн активных пользователей

Создатели социальной сети Pinterest официально заявили, что сегодня база ежемесячных активных пользователей превышает 250 млн человек (InternetUA).

Более 80 % пользователей Pinterest живут за пределами США. Сегодня в Pinterest уже более 175 млрд записей. По сравнению с началом 2017 года объем контента увеличился на 75 %.

Свежее исследование, проведенное Nielsen, указывает на то, что 98 % пользователей Pinterest стараются реализовать найденные в этой сети идеи в реальной жизни. У других социальных сетей этот показатель составляет 71 %.

***

16.09.2018

Новая профессиональная соцсеть работает по принципу Tinder

В мире, где связи решают все, почти не осталось места для личных встреч. Мы все чаще проводим онлайн-конференции и все важные вопросы предпочитаем решать посредством сообщений, реже – звонков. Тем не менее, новое приложение Shapr предлагает не просто обзаводиться профессиональными контактами, но и «выйти из комнаты», чтобы проводить деловые встречи с новыми знакомыми оффлайн (Телекритика).

Сеть личных контактов – это главная ценность журналиста и важный источник инфомации. Приложение Shapr позволит расширить эту сеть. Оно сочетает в себе функции профессональной соцсети LinkedIn и приложения для знакомств в Tinder. Вы точно так же можете «свайпнуть» вправо понравившийся профиль и влево тот, который вас не заинтересовал.

Единственное и главное отличие – в Shapr вы ищете не пару, а профессионалов из любой нужной вам сферы. Здесь работает принцип Tinder – только в случае взаимной симпатии или заинтересованности, вы получите возможность связаться с контактом и договориться о встрече.

В выборе пользователей вам помогут тэги с описанием профессиональных навыков, описание профилей и схожие интересы и амбиции.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

6.09.2018

Менше чверті депутатів Полтавської міськради комунікують з виборцями в соцмережі

Наразі наймасовішою в світі і законною в Україні соцмережею є Facebook. Тож, чи користуються депутати Полтавської міської ради цією соціальною мережею, аби спілкуватися зі своїми виборцями?

Докладніше

***

7.09.2018

В Україні запустили для аграріїв флешмоб – #GoЗаАгроДотаціями

Агросектор за 8 місяців отримав менше 10 % дотацій із 6,3 млрд грн держпідтримки закладеної у бюджет на цей рік. Про це йдеться у матеріалі AgroPolit.com «GoЗаАгроДотаціями» в рамках проекту «Абетка Агродотацій».

Видання проаналізувало усю інформацію, розміщену на офіційному сайті Мінагрополітики, КМУ та у відкритому доступі та з'ясувало, що до АПК дійшло тільки 459 млн грн! «На початку року голова уряду Володимир Гройсман наввипередки з в.о. аграрного міністра Максимом Мартинюком публічно звітували про фінансове покращення для агросектору на 2018 рік. Намалювали гарні презентації з 6,3 млрд грн, а фактично за 8 місяців виділили реально з бюджету аграріям пшик! Інакше й не назвеш ці 459 млн грн», – сказано у статті.

«AgroPolit.com запускає флешмоб #GoЗаАгроДотаціями і закликає всіх аграріїв прийняти участь в ньому… Лишилося 4 місяці, а казна винна АПК 5.8 млрд грн дотацій… Ви сплатили ці гроші у вигляді податків у бюджет і маєте повне право на них...», – сказано у матеріалі.

***

10.09.2018

Днепряне в соцсетях проводят флешмоб «Обними ребенка»

Ежегодно 10 сентября отмечается Всемирный день предотвращения самоубийств. Сотрудники правоохранительных органов Днепра и области предложили провести необычный флешмоб в соцсетях: «Обними ребенка» (49000.com.ua).

Эта идея родилась у работников правоохранительных органов и родителей, которые обращаются к ним, сообщает пресс-служба Днепровского горсовета.

Флешмоб «Обними ребенка» имеет целью напомнить днепрянам о важности такого контакта с детьми. Принять участие в акции может каждый желающий. Для этого нужно обнять ребенка и сфотографироваться, а затем разместить фото с хэштегом # обіймидитину в соцсетях.

Управление-служба по делам детей департамента социальной политики Днепровской городского совета, управления-службы по делам детей районных в городе советов и подчиненные департаменту социальной политики горсовета коммунальные учреждения социальной защиты детей уже присоединились к этой акции и зовут всех неравнодушных также поучаствовать.

***

10.09.2018

В Запорожье организовывают несколько флешмобов против выбросов

В соцсети сразу несколько людей организовывают флешмобы против выбросов. Так, один из пользователей предлагает делиться фото подоконников, на которых собирается промышленная пыль, а известный общественник и бывший заммэра Бердянска Вадим Тихонов предлагает не ограничиваться соцсетью и провести общегородской флешмоб (ZaБор).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

4.09.2018
Instagram задает новые тренды на рекламном рынке

Бренды начинают тратить все больше денег на рекламу в Instagram Stories и создание вертикальных видеороликов под формат – об этом свидетельствуют данные, которые представил ресурс Digiday (Prportal).

По информации источника Digiday, расходы компаний на рекламу в Instagram Stories увеличились на 23 % во втором квартале 2018-го года. Формат Stories привлек больше рекламодателей к Instagram. Также средняя стоимость за тысячу показов в первые полгода 2018-го составила $ 4,91 долларов, говорится в анализе Brand Networks.

Эксперты утверждают, что покупка объявлений в Instagram Stories обходится рекламодателям зачастую дешевле, чем в Facebook. И хотя посты в ленте набирают больше охватов, чем в Stories, последние компенсируют этот недостаток тем, что рекламное объявление занимает весь экран пользовательского смартфона. Также отмечается, что 72 % пользователей соцсети досматривают рекламу в Stories до конца, что является очень высоким показателем вовлеченности. Для сравнения, осенью 2017 года эта цифра достигала 64 %.

Instagram активно привлекает молодую аудиторию. Так, 68 % миллениалов смотрят истории в Instagram, показатель просмотров аналогичного контента в Snapchat – 49 %.

«Если вы на мероприятии и хотите поделиться этим со своими друзьями, разместите ли вы пост в своей ленте? Скорее всего, вы поделитесь этим в истории», – уверена Лиа Форсайт, управляющий директор независимого творческого агентства HarrimanSteel.

Форсайт отмечает, что преимущество Isntagram кроется в количестве инструментов соцсети, позволяющих дополнять историю стикерами, gif-анимацией, опросами, голосованиями и прочими средствами выражения.

***

5.09.2018
Instagram разрабатывает отдельное приложение для покупок
Вадим Карпусь

Специалисты соцсети Instagram в настоящее время работают над созданием нового отдельного приложения, предназначенного для совершения покупок. Оно может получить название IG Shopping (ITC.ua).

При помощи нового приложения пользователи смогут просматривать коллекции товаров от тех торговых площадок, на которые они подписаны. Если какой-то товар понравится, его можно будет купить прямо в приложении. О таких планах рассказали два осведомлённых человека, но сама соцсеть Instagram отказалась комментировать эту информацию.

Пока нет сведений о том, когда следует ожидать презентацию нового приложения IG Shopping, так как его разработка всё ещё продолжается. Кроме того, нельзя исключать возможности полного отказа от выпуска такого приложения.

На текущий момент в Instagram насчитывается более 25 млн коммерческих учётных записей, и 2 млн из них являются рекламодателями. Около 80 % пользователей соцсети подписаны как минимум на одну коммерческую учётную запись. Создание отдельного приложения позволит Instagram удовлетворить запросы своих клиентов, а заодно увеличить собственный доход. А в дальнейшем Facebook сможет предоставить и дополнительные инструменты для продавцов, развивающих свой бизнес в рамках платформы Instagram.

***

8.09.2018

Facebook откроет первый дата-центр в Азии

Facebook планирует открыть первый азиатский дата-центр. Компания построит специальное 11-этажное здание, которое расположится в Сингапуре (InternetUA).

Как отметили представители Facebook, дата-центр позволит сервисам работать быстрее и эффективнее. Проект обойдётся компании в $1 млрд, при этом строительство будет полностью вестись за счёт возобновляемых источников энергии. Кроме того, Facebook намерена использовать новую системную технологию StatePoint Liquid Cooling, которая должна минимизировать потребление воды и электроэнергии.

Новый дата-центр, по словам компании, предоставит сотни рабочих мест и «станет частью растущего присутствия Facebook в Сингапуре и Азии». Стоит отметить, что в Азиатско-Тихоокеанский регионе насчитывается 894 млн пользователей, что составляет 40 % от общего числа базы юзеров.

Как сообщалось ранее, Facebook – не первая компания, размещающая даты-центры в Азии. У Google уже имеются два в Тайване, а недавно компания объявила о намерении построить третий в Сингапуре.

***

12.09.2018
Ирина Фоменко
Google, Facebook и Amazon монополизируют Интернет

Крупные технологические компании, такие как Alphabet и Facebook, подавляют конкуренцию и должны быть расформированы. Об этом сообщает CNBC (InternetUA).

По мнению директора Annenberg Innovation Lab Джонатана Таплина, поскольку эти отраслевые предприятия монополизируют Интернет и диверсифицируют свой бизнес, их нейтралитет находится под пристальным наблюдением.

Таплин, бывший вице-президент по медиасделкам по слиянию и поглощению в Merrill Lynch, указал на важное решение Европейского союза: в качестве примера оштрафовать Google на 2,7 млрд долларов за нарушение антимонопольного законодательства.

Регуляторы обнаружили, что поисковый гигант следует только своим рекомендациям, а не советам от третьих лиц, таких как Yelp. «Это серьезная проблема, поскольку Amazon, например, планирует заняться бизнесом по производству собственных продуктов», – прокомментировал Таплин.

Facebook столкнется с аналогичными проблемами, поскольку компания планирует реализовывать прямые трансляции спортивных соревнований. Недавно социальная сеть получила право на показ матчей Премьер-лиги в некоторых странах Юго-Восточной Азии и в матчах Ла Лиги в Индии. Такие шаги Facebook демонстрируют тот факт, что цифровые платформы все чаще входят в телевизионный бизнес.

«Если бы Facebook продал Instagram, а Alphabet – YouTube, цифровой мир изменился бы к лучшему. Но это вряд ли произойдет в США», – заявил Таплин. – «Таким крупным компаниям будет сложно приобрести еще одно большое предприятие».

Недавняя покупка Amazon Whole Foods не вызвала серьезного неодобрения, однако если Google попытается купить Spotify, такую сделку заморозят.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

3.09.2018

Гра «Момо»: що це таке і що потрібно знати про нову смертельну гру для підлітків

Катерина Петренко

Нещодавно у мережі з'явилась моторошна розвага «Момо», що провокує самогубство дітей зі слабкою психікою, на кшталт суїцидальної гри «Синій кит». Імовірно, вона вже підбирається до України.

Докладніше

***

5.09.2018

Телефон станет вашим психологом: эти приложения помогут в самой сложной ситуации

Еще в прошлом году использование приложений для смартфонов, связанных со стилем жизни, возросло на 174 %. Среди таких приложений на загрузочных платформах типа Play Market или App Store отдельное место занимают психологические сервисы. Об этом рассказала психолог Марина Дворник (Politeka).

«Чаще всего – это что-то вроде электронных книг по самопомощи. Благодаря им можно подробнее почитать об агрессии, тревожности, депрессии, самооценке, стрессе, оценить собственные симптомы и воспользоваться рекомендациями по освоению тяжелых состояний», – сообщает Марина Дворник.

Например, мобильное приложение «What's Up?» содержит удобно организованную информацию и мотивирующие цитаты. Оно также позволяет вести дневник своих настроений и положительных и отрицательных привычек.

«Функция мониторинга эмоций – это еще один наиболее распространенный инструмент самопомощи. Благодаря приложениям «Daylio» и «Puncher» можно понять, какие виды повседневной активности сопровождают определенные эмоции. Можно запланировать чаще делать то, что вдохновляет, а не подавляет, и отслеживать изменения».

«Один из разновидностей смартфон-приложений психологического направления – чаты. Там можно поделиться своим осложнением и программа начнет "переписываться" с Вами, чтобы как можно лучше понять потребности. По такому принципу работают приложения Youper и Woebot, обучая пользователя основам конструктивного мышления и контроля своих переживаний», – информирует Марина Дворник.

Стоит выделить приложение Vivian: Free Personal Psychotherapist, в котором представлена виртуальная 3-D версия психотерапевта. Этот бот имитирует ситуацию настоящего общения. Через анализ аудиосообщений программа предоставляет почти моментальные голосовые ответы.

***

5.09.2018

Стали известны новые жертвы опасной подростковой суицидальной игры Momo

Жертвами новой суицидальной «игры» Momo стали двое подростков из Колумбии. Как выяснили журналисты «Фразы», по данным СМИ, на днях там покончили с собой два школьника из Колумбии – 12-летняя девушка и 16-летний юноша (InternetUA).

Как сообщает Daily Mail, подростки были знакомы, и именно он втянул свою подругу в эту «игру», в которой зловещий персонаж давал игрокам задания в мессенджере WhatsApp. Последним из них стал приказ покончить с собой. В случае невыполнения задания ребятам грозило некое «темное проклятие».

Первым было найдено тело парня. В течение 48 часов она также была найдена мертвой. Местные СМИ утверждают, что тело, повешенное в шкафу, нашли родственники.

В изъятых телефонах полиция обнаружила сообщения, связанные с игрой. Эту информацию подтвердил представитель колумбийского правительства Ханьер Ландоно.

Утверждается, что это первые жертвы этой игры в Колумбии.

***

7.09.2018

Украинцам рассказали, как защитить своих детей от новой интернет-страшилки

Специалисты рассказали украинцам, как защитить своих детей от новой интернет-страшилки MOMO. Об этом сообщают украинские журналисты (InternetUA).

«Идут реальные угрозы. Угрозы физической расправы. Либо самому подростку, либо его родителям и семье. Они, как правило, однотипны: я знаю, где ты живешь, знаю где работают твои родители и так далее», – сказала эксперт по безопасности детей Елена Лизвинская.

В то же время специалист в сфере IT Максим Самойленко утверждает, что ради дополнительной безопасности, украинцы могут начать бороться со страшилкой вполне реальными техническими средствами.

«Это опасно. Это спам, а дети воспринимают как руководство к действию. Первое, что нужно сделать – это заблокировать все сообщения от незнакомых контактов. Второе – ограничить доступ к социальным сетям», – подчеркнул он.

Также специалисты рекомендуют поставить на телефон специальную программу для контроля за контентом и объяснять детям, что данные в наше время являются общедоступными.

«Объясняйте детям, что информация о том, кто и где живет, где работают родители и так далее – общедоступна», – сказала Лизвинская, пишет politeka.net.

***

11.09.2018

Видео «фейковых» самоубийств заполонили YouTube

Издание The Sun обвинило популярный видеохостинг YouTube в заработке на шокирующих видео с фейковыми самоубийствами. Эти видео порой набирают на ресурсе до 35 миллионов просмотров (Інфотаб).

Об этом пишет Корреспондент.

По данным издания, на сегодняшний день самоубийства забирают наибольшее количество жизней людей, не достигших 35-летнего возраста. Каждый пятнадцатый британец совершал попытку убить себя. При этом каждые 90 минут в Британии такая попытка заканчивается смертью.

Популярный таблоид заявляет, что YouTube зарабатывает на шокирующем контенте, где пранкеры притворяются, что совершают самоубийства. Авторы издания обнаружили сотни подобных видео, из которых некоторые набрали миллионы просмотров.

Благотворительные организации по охране психического здоровья предупредили The Sun, что эти видеоролики могут даже вдохновлять на настоящие самоубийства из-за методов, показанных в некоторых клипах.

***

10.09.2018

Як Facebook спростив людьське спілкування

Онлайн-сервіси потребують контенту, який можна легко класифікувати. Це вплинуло і на людей. Письменник та колишній інженер Microsoft та Google Девід Аувербах (David Auerbach) пояснив як інтернет змінює сучасне спілкування. Якщо у двох словах, то люди змушені реагувати на контент простими діями, що, у свою чергу, поєднує людей та сприяє спілкуванню.

Докладніше

***

12.09.2018

Суїцидальна гра «Момо»: підліток з Полтавщини видавав себе за «куратора»

В Україні не зафіксовано жодного випадку, коли б діти травмували себе внаслідок участі у так званій «суїцидальній грі Момо». Крім того, деякі підлітки розважаються, пишучи повідомленні від «Момо» (Espreso.tv).

Про це повідомляє речниця кіберполіції Юлія Квітко на своїй сторінці у Facebook.

Зазначається, що до поліції не надходило жодного офіційного звернення про такі випадки. Вся інформація, яка була поширена деякими ЗМІ в мережі, про нібито «слід МОМО» в дитячих суїцидах, не знайшла свого підтвердження.

«Діти ж бачать всі ці сюжети по ТВ і в мережі Інтернет та, не розуміючи наслідків своїх дій, жартують таким чином над своїми однокласниками та знайомими. Як приклад, додаю переписку з псевдо-“Момо”, який виявився підлітком з Полтавщини. Тож давайте не сіяти паніку там, де її немає», – написала Квітко.

***

12.09.2018

Черное зеркало: как побороть зависимость от соцсетей, пока не поздно

Насколько опасно повальное увлечение людей смартфонами? Ни для кого не секрет, что чрезмерное пользование гаджетами и социальными сетями ведет к разрушению социальных контактов и возникновению зависимости, однако ученые все еще не могут определить, существует ли в действительности эта зависимость.

Докладніше

Маніпулятивні технології

4.09.2018

Генпрокуратура РФ звинувачує Google у «втручанні у вибори»

Генпрокуратура Росії винесла Google застереження про «неприпустимість втручання у російські вибори» (Укрінформ).

Про це заявив заступник начальника управління з нагляду за виконанням законів про федеральну безпеку Генпрокуратури РФ Олексій Жафяров, повідомляє РІА «Новини».

При цьому чиновник додав, що застереження не вимагає реакції з боку компанії. «Але це (винесення попередження Google – ред.) досить серйозна міра, за якою вже слідує притягнення до встановленої законом відповідальності», – сказав Жафяров.

Повідомляється, що претензії до компанії висловили також ЦВК і Роскомнагляд. Вони надіслали в Google офіційні листи, де звинувачують компанію у «рекламі незаконних акцій у день виборів».

За словами заступника голови Роскомнагляду Вадима Субботіна, десятки спеціалізованих YouTube-каналів «ведуть масовані акції», закликаючи порушувати закон.

Імовірно, російські відомства мають на увазі YouTube-канали російської опозиції, у першу чергу, Навальный-Live. Опозиціонер Олексій Навальний зі своїми прихильниками закликав в єдиний день виборів у РФ 9 вересня провести по всій країні масові акції проти підвищення пенсійного віку.

У ЦВК і Роскомнагляді відзначили, що американське відділення компанії не відповіло на листи.

Як відомо, 9 вересня у РФ пройде єдиний день голосування.

***

4.09.2018

Британські медіа закликали уряд моніторити контент соцмереж

Керівники відомих британських ЗМІ і телекомунікаційних компаній закликали уряд країни ввести незалежний нормативний нагляд за інформацією в соціальних мережах (Prportal).

Про це йдеться в відкритому листі, який підписали BBC, Sky, ITV, Channel 4, BT та TalkTalk, повідомляє Media Sapiens із посиланням на Financial Times.

Підписанти зазначають, що інтернет надає багато хороших можливостей, однак, як і всі медіа, він може нести загрози. Зокрема йдеться про дитячу експлуатацію, вплив фейкових новин на політику, психічне здоров'я дітей та інші небезпеки.

Суспільні та приватні компанії, які підписали листа, не вважають «реалістичним чи доцільним», аби лише самі інтернет-компанії на кшталт Facebook чи Google вирішували, який контент є прийнятним. Вони переконані, що для цього потрібний також незалежний регулятор.

«Мова йде не про цензуру, а про те, щоб зробити інтернет безпечнішим, забезпечуючи звітність і прозорість рішень, які приймають ці приватні компанії», – наголошується у зверненні.

Раніше Ofcom, регуляторний орган у сфері медіа та телекомунікацій Великої Британії, повідомляв, що не має повноважень боротися зі шкідливим онлайновим контентом. Тепер очільниця Ofcom Шерон Вайт публічно заявила, що підтримує ідею незалежного регуляторного контролю контенту технологічних компаній, які публікують новини.

***

5.09.2018

Очільник розвідки США попередив про кіберзагрози «з декількох країн» для майбутніх виборів

Четвертого вересня голова національної розвідки США Ден Коутс заявив, що він занепокоєний інформацією про кіберзагрози щодо майбутніх виборів у США, які «надходять з декількох країн», передає УНН з посиланням на Reuters.

Очільник нацрозвідки заявив під час виступу на Саміті розвідки та національної безпеки в штаті Меріленд, що під час цьогорічних виборів до Конгресу США, які пройдуть в листопаді, є загроза зовнішнього втручання, так само як і в президентські вибори 2020 року.

«Наша взаємозалежність полегшує нашим ворогам здійснення операцій з використанням деструкційної інформації , щоб посіяти розбрат і підірвати нашу демократію та наші цінності, як ми це бачили під час зусиль Росії та інших країн», – заявив Коутс.

***

6.09.2018

Диктаторы заточили Facebook под себя

Ирина Фоменко

В прошлом месяце Facebook обнаружил доказательства скоординированной кампании влияния на своей платформе, во главе которых стоят иранские группы. Четвертого сентября несколько исследований пролили свет на другие способы, используемые правительствами в Facebook в ужасных целях: создание бригад влиятельных людей и платных армий троллей для подавления инакомыслия и отрицания реальности злодеяний в области прав человека. Об этом сообщает The Verge.

Докладніше

***

5.09.2018

У соцмережах розгортається «гонка озброєнь» – операційний директор Facebook

Втручання Росії у виборчий процес в США було неприпустимим нападом на цінності країни, і компанія Facebook докладатиме зусиль, аби подібне не повторилося. Про це заявила головний операційний директор Facebook Шеріл Сендберг під час слухань на тему використання платформ соціальних мереж в іноземних операціях впливу.

Докладніше

***

5.09.2018

В Facebook рассказали, что подготовились к вмешательству в выборы

В интернет-компании Facebook подготовились к возможному иностранному вмешательству в выборы, в том числе в промежуточные выборы в США, которые состоятся в ноябре 2018 года, рассказал американский телеканал NBC News.

Докладніше

***

6.09.2018

Представник Twitter вперше постав перед сенаторами через пропаганду

Одна з керівників Facebook Шеріл Сандберг і гендиректор Twitter Джек Дорсі виступили на слуханнях комітету з розвідки сенату США (Інформатор).

Роботою найбільшої соцмережі світу сенатори вже цікавилися, а от Twitter відповідав на запитання політиків вперше, – пише ББС Україна.

Генеральний директор Twitter Джек Дорсі та головний виконавчий директор Facebook Шеріл Сандберг говорили про цензуру та використання соціальних мереж для поширення політичної пропаганди.

В Америці проводять розслідування щодо можливого втручання Росії у вибори в США за допомогою поширення фейкових новин та дезінформації під час президентської кампанії у США 2016 року. У квітні з цього приводу в сенаті виступав творець Facebook Марк Цукерберг.

Сенатори хочуть переконатися, що ситуація із закордонним втручанням не повториться у листопаді під час проміжних виборів. Вони хотіли послухати і керівників Google, але від них ніхто не прийшов.

У Google хотіли відправити на слухання старшого віце-президента і головного юриста компанії Кента Вокера, але сенатори бажали бачити лише очільника Сундара Пічаї або гендиректора материнської структури Alphabet Ларрі Пейджа. Зрештою місце, підготоване для Google, лишилося порожнім, що розчарувало сенаторів.

Голова сенатського комітету Річард Берр на початку засідання нагадав про роль, яку інтернет-сервіси зіграли під час передвиборчої кампанії 2016 року у США. Москва своє втручання у вибори в США спростовує. У Вашингтоні ж вважають, що до цього може бути причетна так звана «фабрика тролів».

***

15.09.2018

Жители КНДР создавали фейковые аккаунты в соцсетях из-за санкций

Жители Северной Кореи создавали фейковые аккаунты в соцсетях, чтобы находить работу в обход американских санкций, сообщает The Wall Street Journal (InternetUA).

Отмечается, что подобные схемы использовали россияне, которые таким образом якобы вмешивались в американские президентские выборы.

Жители КНДР притворялись гражданами другой страны, например, Японии, и искали удаленную работу на специальных сервисах. При этом

общались с клиентами они через мессенджеры, а оплату получали через онлайн-кошельки.

Изданию удалось получить данные с порталов по поиску работы и поговорить с рядом клиентов. По данным WSJ, северокорейцы могли заработать несколько десятков тысяч долларов на разработке программного обеспечения.

Спецслужби і технології «соціального контролю»

3.09.2018

«ВКонтакте» лишила пользователей возможности удалить всю информацию о себе

«ВКонтакте» обновила правила, после чего из них исчезла фраза о том, что удаление персональной страницы означает автоматическое удаление всей размещенной на ней информации (InternetUA).

По данным издания, правила ВК обновились 3 сентября. В частности, изменился пункт 8.7, в котором ранее было написано, что «удаление персональной страницы пользователя означает автоматическое удаление всей информации, размещенной на ней, а также всей информации пользователя, введенной при регистрации на сайте».

Сейчас пункт 8.7 гласит, что «удаление персональной страницы пользователя означает удаление данных пользователя и всей информации, размещенной на ней, за исключением данных, временное хранение которых необходимо в соответствии с действующим законодательством Российской Федерации».

В «ВК» сообщили, что обновление правил имеет технический характер, заверив, что «никаких существенных изменений для пользователей не произошло». «Русская служба Би-би-си» отмечает, что англоязычная версия правил «ВК» не изменилась.

***

3.09.2018

Президент Египта ужесточает контроль за соцсетями

Президент Египта Абдель Фаттах эль-Сиси ратифицировал закон, предоставляющий властям право контролировать пользователей социальных сетей в стране в рамках ужесточения интернет-контроля (Аспекты).

Утвержденный парламентом в июле, государственный Верховный совет по регулированию СМИ будет обладать полномочиями наблюдать и контролировать людей, чьи аккаунты в соцсетях или блогах имеют более 5000 последователей.

Совет уполномочен приостановить или заблокировать любой личный аккаунт, который «публикует или транслирует фейковые новости или материалы, подстрекающие к нарушению закона, насилию или ненависти».

***

4.09.2018

Блокування сайтів: скандальний закон вирішили зробити ще крутішим

В Україні розгорівся скандал після анонсування законопроекту, згідно з яким спецслужби зможуть блокувати інтернет-ресурси до судового рішення, якщо вважатимуть за потрібне. Комітет інформації і зв'язку ВР відправив документ №6688 на доопрацювання (Znaj.ua).

У ході засідання глава комітету Олександр Данченко заявив, що «дуже багато норм законопроекту просто прикриваються нацбезпекою, не будучи демократичними і не на захисті прав і свобод».

***

5.09.2018

WSJ: генпрокурор США выясняет, не подавляют ли соцсети свободу слова

Генеральный прокурор США Джефф Сешнс обеспокоен тем, что популярные социальные сети могут подавлять свободу слова. Об этом сообщает The Wall Street Journal (InternetUA).

По данным издания, Сешнс намерен провести встречу с генеральными прокурорами штатов, чтобы обсудить ситуацию вокруг соцсетей в США.

Как отмечается, Сешнс планирует выяснить, могут ли Facebook и Twitter вредить конкуренции и намеренно подавлять свободный обмен идеями.

При этом минюст США уже занимается расследованием данной проблемы.

***

10.09.2018

Мининформполитики «открестилось» от бана Facebook-страницы блогера Шария

Министерство информационной политики (МИП) Украины отрицает свою причастность к блокированию в социальной сети Facebook как персональной верифицированной страницы журналиста и блогера Анатолия Шария, так и страниц других пользователей (InternetUA).

Об этом говорится в ответе Мининформполитики на запрос Українських Новин.

27 августа информационное агенство Українські Новини запросило у Мининформполитики – обращалось ли данная государственная структура или его подразделения к управляющей компании соцсети Facebook с просьбами или предложениями забанить персональные страницы пользователей, которые несут информационную угрозу Украине, в том числе Facebook-страницу блогера Анатолия Шария?

«В рамках реализации Доктрины информационной безопасности Украины, утвержденной указом Президента Украины от 25 февраля 2017 года №47/2017, МИП начало диалог с администрацией социальной сети Facebook. В частности, в июле этого года состоялась встреча заместителя министра информационной политики Дмитрия Золотухина с ведущим специалистом компании по вопросам политики социальной сети в сфере контртерроризма Д-р Эрин Мари Салтман и руководителем направления политики Facebook в Центральной и Восточной Европе Габриелой Чех. Ключевым вопросом встречи было совершенствование политик Facebook и их имплементация», – говорится в ответе министерства.

«Главной целью диалога МИП и Facebook является формирование эффективных и объективных стандартов и методик анализа информации. МИП информирует администрацию Facebook (как, например, в случае с верификацией страниц субъектов властных полномочий), которая, в свою очередь, принимает собственное – исключительно собственное, без какого-либо влияния со стороны МИП – решение о распространяемой информации», – подчеркнули в Мининформполитике.

***

7.09.2018

Грабили иностранные банки: СБУ накрыла банду хакеров

Сотрудникам СБУ удалось разоблачить международную хакерскую группу, которая занималась хищением и легализацией денег, снятых со счетов банков из более двадцати стран мира, передает пресс-служба ведомства (InternetUA).

Преступники использовали специальное программное обеспечение, которое позволяло им получать доступ к данным юрлиц банков из стран ЕС, Южной Азии и постсоветского пространства. После этого они создавали в банковских системах липовые платежки и с их помощью выводили средства.

Легализировали деньги преступники через несколько фиктивных финансовых операций с фирмами-посредниками, часть из которых была подконтрольна российским спецслужбам. Каждый из участников сделки получал оговоренный процент от суммы похищенных средств.

Во время обысков по местам жительства участников группировки в Киеве, Черновцах, Одессе и Вознесенске СБУ изъяла документацию, которая подтверждает факты подделки банковских гарантий и незаконное перечисление похищенных денежных средств через популярные банковские системы.

«Сотрудники СБУ также обнаружили электронное письмо, которое доказывает легализацию похищенных средств, в частности через контрагентов, связанных со спецслужбами РФ», – говорится в сообщении.

Во время операции был задержан организатор группы – гражданин одной из стран Ближнего Востока и его сообщник.

***

11.09.2018

Слежка за лайками. НАБУ хочет мониторить соцсети за 42 тысячи гривен

Виталий Губин

Национальное антикоррупционное бюро объявило о закупке услуг по мониторингу и анализу социальных сетей, а также по изучению медиа-активности в региональных СМИ, посвященных упоминаниям ведомства. Соответствующие заявки, датированные 6 сентября, размещены на портале публичных закупок Prozorro.

Докладніше

***

10.09.2018

У Росії можуть з'явитися суди для розгляду «злочинів» у соцмережах

На території Російської Федерації можуть створити спеціальні суди, у яких розглядатимуть справи, пов'язані з соцмережами і цифровим правом (Український інтерес).

Таку заяву спецпредставника президента РФ із цифрового і технологічного розвитку Дмитра Пєскова цитують росЗМІ.

«Практика кримінальних справ за репости і лайки показала, що нинішня судова система тут працює не дуже ефективно», – сказав він.

Пєсков вважає, що активні дії в онлайн-сфері загрожують суспільству. Йдеться, зокрема, і про маніпулювання свідомістю користувачів. Він підкреслив, що замість чинної системи потрібний «гарно налаштований оцінний механізм».

«Мені здається, те, як це відбувається сьогодні, працює не дуже ефективно. Зважаючи на те, як розвивається цифрове право, я допускаю і появу спеціалізованих інституцій», – заявив спецпредставник президента РФ.

***

11.09.2018

Військовим РФ хочуть заборонити публікувати дані про себе в соцмережах

Уряд Росії вніс в Держдуму законопроект, що забороняє військовослужбовцям цієї країни розміщувати в інтернеті та ЗМІ дані про себе і своїх товаришів по службі (Hromadske).

Відповідний документ опублікований на сайті Держдуми РФ.

Як випливає з документу, військовослужбовцям пропонують заборонити розміщувати у ЗМІ та інтернеті відео та фото, дані геолокації, а також будь яку іншу інформацію про себе і інших військовослужбовців, які дозволять «розкрити відомчу приналежність».

Забороняється також публікувати дані про військові частини, організації і підрозділи, в яких силовики проходять військову службу, а також місце їхньої дислокації.

За порушення передбачених заборон військових зможуть притягнути до дисциплінарної відповідальності. Це також може стати основою для дострокового звільнення силовиків.

Наголошується, що при роботі над законопроектом «був використаний зарубіжний досвід». Зазначається, що закон не буде поширюватися на «громадян, звільнених з військової служби».

Зазначимо, російські військові неодноразово публікували свої фото та відео в соцмережах, при цьому, вказуючи геолокацію. Це дозволяло розслідувачам вирахувати позиції військових РФ, які були причетними до бойових дій на Донбасі.

***

12.09.2018

СБУ разоблачила администратора антиукраинских групп в соцсетях

Сотрудникам СБУ удалось разоблачить в Прилукском районе Черниговской области администратора антиукраинских сообществ в различных социальных сетях, передает пресс-служба ведомства в Facebook (InternetUA).

Мужчина занимался созданием в соцсетях аккаунтов, через которые он распространял антиукраинскую информацию и материалы с призывами к изменению границ территории страны, свержению конституционного строя и государственной власти.

Также он пропагандировал деятельность так называемых «ЛДНР» и дискредитировал ВСУ.

Во время обысков у мужчины правоохранительные органы нашли компьютеры и несколько мобильных устройства.

Действия злоумышленника квалифицированы по ст. 110 (Посягательство на территориальную целостность и неприкосновенность Украины) УК Украины.

***

13.09.2018

Начальник спецотдела ФСБ рассказал ФБР о работе российских ботов

Игорь Козлов

12 сентября в федеральном суде Хартфорда дал признательные показания гражданин России Петр Левашов. 38-летний житель Санкт-Петербурга обвинялся в намеренном повреждении защищенного компьютера, преступном сговоре и хищении личных данных с отягчающими обстоятельствами. Американские СМИ акцентируют внимание на необычности этого дела.

Докладніше

***

14.09.2018

Facebook начал проверку фото и видео на достоверность

Социальная сеть Facebook начала проверку фотографий и видео на достоверность с помощью искусственного интеллекта. Как отмечается в блоге социальной сети, на данный момент она сотрудничает с 27 организациями, которые помогают ей выявлять фейковые новости. Теперь же партнеры Facebook сосредоточатся также на анализе визуальный информации, что поможет быстрее и эффективнее реагировать на появление ложных новостей в социальной сети (Зеркало недели. Украина).

Специально разработанный алгоритм анализирует фото и видео и, если заключает, что какое-либо из них является ложным, отправляет его для изучения специалистам, которые затем смогут заключить, является ли информация, появившаяся на изображении, достоверной. Будут использоваться различные техники анализа изображения, например, обратный поиск или анализ метаданных снимка.

Фейковые фотографии и видео в Facebook разделили на три категории:

– манипулятивные и сфабрикованные;

– вырванные из контекста;

– текстовые или визуальные заявления.

***

15.09.2018

Цукерберг пообещал защиту Facebook от русских хакеров

Основатель и руководитель Facebook Марк Цукерберг заявил, что социальная сеть сейчас в большей степени готова противостоять возможному вмешательству в выборы, чем это было два года назад. Он отметил, что миссия сервиса – «усиливать добро и смягчать вред» (InternetUA).

В США обвиняют Россию в распространении через соцсети дезинформации и фейковых новостей, которые могли повлиять на ход голосования во время президентских выборах в США в 2016 году.

Цукерберг написал в своём блоге, что усилия компании в ту пору были направлены на противостояние традиционным видам кибератак, таким как фишинг, взломы аккаунтов и вредоносные программы. «Мы идентифицировали их и уведомили правительство и пострадавших», – заверил глава Facebook.

«Чего мы не ожидали, так это того, что иностранные пользователи начнут скоординированные информационные атаки через подставные аккаунты, распространяющие раздор и дезинформацию», – признался Цукерберг.

Он напомнил, что соцсеть выявила и удалила сомнительные аккаунты перед выборами в самых разных странах мира. Однако отметил, что несмотря на прогресс, компания по-прежнему сталкивается «с изощренными и хорошо финансируемыми противниками».

«Они не сдадутся и будут продолжать развиваться. Мы должны постоянно совершенствоваться и быть на шаг впереди», – слелал вывод Марк Цукерберг.

***

15.09.2018

Facebook удалила 1,3 млрд поддельных аккаунтов за полгода

За полгода социальная сеть Facebook удалила 1,27 млрд поддельных аккаунтов, сообщила операционный директор компании Шерил Сандберг (Sheryl Sandberg) (InternetUA).

По ее словам, модерация учетных записей проводится как вручную, так и с использованием специальных алгоритмов на основе искусственного интеллекта, машинного обучения и компьютерного зрения.

Штат сотрудников Facebook, которые следят за порядком в социальной сети, вырос вдвое и сейчас составляет более 20 тысяч человек. Они просматривают сообщения более чем на 50 языках 24 часа в сутки, отметила Сандберг.

Facebook активизировала усилия по борьбе с фейковыми аккаунтами, используемых для распространения сфабрикованных новостей и искажения общественного мнения. Кроме того, сервис активно борется со спамом. Так, в январе-марте 2018 года из соцсети было удалено порядка 836 млн рекламных публикаций.

***

17.09.2018

СБУ допомагатиме «Укренерго» та «Укргідроенерго» у кіберзахисті

Служба безпеки України підписала меморандум з енергетичною компанією «Укренерго» та ПАТ «Укргідроенерго» для ефективної системи кібербезпеки.

Докладніше

***

17.09.2018

Исследователи разработали алгоритм, способный выявить экстремиста еще до публикации постов

Группа исследователей из Массачусетского технологического института (MIT) и Университета Брандейса в Массачусетсе разработала алгоритм, который умеет определять экстремистов в соцсетях еще до публикации ими соответствующих постов. Описание алгоритма, созданного на основе анализа нескольких тысяч учетных записей в сети микроблогов Twitter, было опубликовано в журнале Operations Research (InternetUA).

Отметим, что борьба с экстремизмом и разжигающим ненависть контентом является одной из главных и трудных задач для крупных интернет-компаний, включая Facebook, Twitter и YouTube. Власти разных стран требуют от платформ удалять такой контент в максимально сжатые сроки, но сотрудники, занимающиеся модерацией и призванные помогать им автоматические алгоритмы не всегда справляются с задачей. Кроме того, речь в этом случае идет о блокировке и удалении контента после его публикации.

Как пишет N+1, алгоритм американских исследователей, по сути, позволяет осуществлять премодерацию. Он основан на анализе пяти тысяч микроблогов, которые вели члены террористических организаций или связанные с ними пользователи (информация об этих аккаунтах была собрана через СМИ, блоги, аналитиков и правоохранительные органы). Для анализа ученые использовали 4,8 млн твитов, связанных с выбранными акаунтами, описания профилей этих пользователей, а также их друзей и подписчиков (это увеличило базу до 1,3 млн аккаунтов).

На основании этих данных при помощи статмоделирования ученые разработали модель, способную с высокой точностью определить, является ли тот или иной аккаунт экстремистским, до того, как его владелец опубликует первую запись.

По словам одного из соавторов исследования, пользователи, которые занимаются онлайн-экстремизмом, имеют схожие поведенческие характеристики в соцсетях, что и позволяет алгоритму выявлять их при создании новых аккаунтов.

***

17.09.2018

В Росії все частіше саджають за репости в Мережі, – Курносова

В Росії збільшилася кількість кримінальних та адміністративних справ за репости та дописи у соцмережі. Якщо раніше саджали за підтримку України, то наразі – за критику чинної влади.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

3.09.2018

Кіберполіція затримала злочинців, які блокували акаунти в соцмережах за викуп

Основною метою зловмисників було отримання грошей від власників соціальних профілів за повернення доступу до сторінки (InternetUA).

Встановлено, що за допомогою шкідливого програмного забезпечення зловмисники отримували незаконний доступ до електронних поштових скриньок, які були пов'язані з акаунтами жертв. Для цього, на електронні поштові скриньки власників акаунтів соцмережі Instagram здійснювалась розсилка листів, які були інфіковані цим шкідливим програмним забезпеченням. Усі ці листи були замасковані під нібито офіційні повідомлення служби підтримки соціальної мережі.

У подальшому, отримавши доступ, зловмисники вносили зміни до реєстраційних даних, чим блокували доступ справжнім власникам. За повернення доступу вони вимагали від 10 до 30 тисяч гривень у криптовалюті.

Зазвичай, у якості «жертви» обиралися сторінки, кількість підписників яких була більшою 15 тисяч користувачів (сторінки Інтернет-магазинів, відомих людей тощо).

Таким чином зловмисники заволоділи сторінками у соціальних мережах понад тисячі громадян як України, так і іноземців.

За місцем проживання одного із учасників групи проведено санкціоновані обшуки. В ході обшуку поліцейські вилучили комп'ютерну техніку, яку вже направлено на проведення усіх необхідних експертиз.

За даним фактом розпочато кримінальне провадження за двома статтями Кримінального кодексу України: ч.2 ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч.3 ст.190 (Шахрайство). Зловмисникам загрожує до восьми років позбавлення волі.

***

3.09.2018

MasterCard передає дані про покупки клієнтів Google – Bloomberg

Інтернет-гігант Google і платіжна система MasterCard уклали таємну угоду про передачу історії фінансових трансакцій користувачів (Економічна правда).

Відзначається, що інформація стосується не лише онлайн-покупок, але і придбання товарів в магазинах роздрібної торгівлі.

Джерела агентства повідомили, що переговори з MasterCard зайняли близько чотирьох років, сума угоди при цьому становила всього 1 млн доларів.

В ході обговорення умов компанії також обговорювали можливість розподілу виручки від реклами. Паралельно з MasterCard інтернет-гігант також вів переговори з іншими платіжними системами, проте поки невідомо, чи вдалося укласти схожі угоди.

Завдяки домовленостям тепер рекламодавці Google можуть отримати можливість аналізувати інформацію про те, чи купували клієнти платіжної системи MasterCard товари, які рекламувалися пошукачем.

Представники компаній відмовилися від коментарів, зазначивши, що особисті дані користувачів ніколи не розкривалися.

***

3.09.2018

Уряд Німеччини створює нове агентство з кібербезпеки

Уряд Німеччини схвалив рішення про створення нової структури з кібербезпеки для посилення захисту країни – Агентстві з питань інновацій у сфері кібербезпеки (Еспресо).

Про це повідомляє Defense News.

Нову організацію спільно очолюють міністри оборони та внутрішніх справ. Агентство отримає бюджет в розмірі 200 млн євро в період між 2019 та 2022 роками. У новому агентстві працюватимуть близько 100 співробітників.

Німецький парламент обговорюватиме пропозицію щодо затвердження роботи агентства найближчим часом. Щойно фінансування буде схвалено, аналітики почнуть свою роботу з наступного року.

Однією з цілей нового агентства є прискорення циклу виробництва технологій кібербезпеки.

«Існуючі урядові процеси, що стосуються досліджень, є занадто повільними. Ми повинні бути принаймні такими ж швидкими і добре оснащеними, як і злочинці», – сказала міністр оборони Урсула фон дер Ляєн.

Очікується, що завдяки агентству урядові структури володітимуть продуктом для аналізу загроз та можливого віртуального удару у відповідь та не будуть змушені чекати його появи на ринку і купувати.

У створенні відомства Німеччина орієнтується на відповідні державні агенції США та Ізраїлю.

***

4.09.2018

Миллионы пользователей WhatsApp в опасности

Недавно аудитория мессенджера WhatsApp превысила отметку в 1,6 млрд человек. Все эти люди с помощью данного сервиса общаются, используя для этого различные виды данных (InternetUA).

Как удалось выяснить 4 сентября, миллионы пользователей, использующих этот сервис, находятся прямо сейчас в страшной опасности. Из-за нее вся личная информация может попасть в руки третьих лиц, но речь даже не о переписке, а о фотографиях.

Стоит ли лишний раз говорить о том, что будет, если в руки злоумышленникам попадут чьи-то личные фотографии с привязкой к конкурентному человеку. По данным экспертов из антивирусной компании ESET, для операционной системы Android недавно было выпущено новое шпионское ПО, которое маскируется под Viber.

Тем не менее, из-за него происходит рассекречивание личной информации и снимки из мессенджера WhatsApp попадут в руки злоумышленников с привязкой к номеру телефона.Пользователей смартфонов на базе Android в настоящее время активно перенаправляют на ресурс, который маскируется под Google Play. В нем предлагается установить мессенджер Viber, однако, конечно, в результате этого на мобильное устройство попадет вредоносное ПО.

После этого оно запросит все необходимые права, а затем начнет искать в памяти мобильного устройства все фотографии и прочие медиафайлы, которые в ней имеются. В ходе эксперимента, проведенного специалистами по безопасности, вредоносное программное обеспечение украло лишь снимки из WhatsApp, которые в памяти телефона на базе Android хранятся со специальными пометками.

Другая информация с мобильного устройства не похищается, хотя программному обеспечению выдают разрешение на доступ к контактам, отправку сообщений и совершение звонков, а также на многие другие вещи. Чтобы не стать жертвой вымогателей денег достаточно просто не устанавливать вредоносное ПО по ссылкам в браузере.

***

4.09.2018

Блокчейн-стартап хочет победить сетевых троллей с помощью распознавания лиц

С помощью Trollteq любой сайт может проводить идентификацию пользователей и не давать и регистрироваться снова, если они попадут в бан. Разработчики утверждают, что юзеры смогут сохранить анонимность, хотя им и придется раскрыть свой ID (InternetUA).

Молодая компания Authenteq, у которой есть офисы в Исландии, Германии, Великобритании и США, разработала предложение для владельцев сайтов, которые хотят искоренить интернет-троллей на своей платформе. Авторы Trollteq предлагают способ идентификации пользователей, при котором личные данные будут защищены блокчейном.

Весь процесс идентификации займет у пользователя около 90 секунд. Его попросят сфотографироваться и прислать скан документа, удостоверяющего

личность, для распознавания лица. Как только Trollteq убедится, что регистрацию прошел реально существующий человек, он сообщит об этом владельцу сайта – своему заказчику. При этом компания не раскроет личность юзера.

«Мы не знаем, кто вы. Но мы знаем, что вы – реальный человек. Такие возможности дарит нам блокчейн», – цитирует VentureBeat директора Authenteq Кари Тора Рунарссона.

Стартап уверяет, что ни создатели базы, ни их заказчики не имеют возможности выдать данные пользователя, даже если к ним официально обратятся власти какой-либо страны.

«Горькая правда заключается в том, что тролли захватили интернет. Наша миссия – лишить их главного ресурса, то есть возможности прятаться за фальшивыми именами, но при этом защитить из право на личную жизнь и свободу слова, – поясняет Рунарссон. – Любой сайт может встроить Trollteq – и мы сможем сканировать миллиарды записей о реальных людях в течение 90 секунд. Это значит, что мы способны работать даже с такой нагрузкой, как в Twitter или Facebook».

***

4.09.2018

На концерт Imagine Dragons в Киеве жулики продали 1000 фальшивых билетов

Мошенники продали ненастоящие билеты на концерт музыкальной группы Imagine Dragons тысяче поклонников (InternetUA).

По информации журналистов, подделки продавали через сайт e-ticket.in.ua, который был широко разрекламирован в поисковиках и социальных сетях. В данный момент сайт уже находится в оффлайне, хотя работал еще в день концерта.

Также, по информации пользователей социальной сети Facebook в группе, созданной специально пострадавшими от мошенничества перед концертом, некоторые поддельные билеты также покупали через «Консьерж Сервис», в свою очередь продающий билеты через свою страницу в сети в Instagram и OLX.

По словам пострадавших, штрих-коды на подделках оказались ненастоящими, а скопированными.

«Только во время самого концерта в полицию отдали заявления 80 человек, я слышала об общей цифре в 1500 пострадавших. В очереди в кризисный центр стояло на глаз около тысячи, но очевидно – не все с этой же проблемой», – говорит одна из пострадавших, приехавшая на концерт из Харькова.

В киберполиции заявляют, что по данному делу уже поступило больше ста заявлений и открыто криминальное производство.

В свою очередь организаторы концерта утверждают, что со своей стороны не имеют никакой возможности вернуть деньги пострадавшим.

***

5.09.2018

Мобільні додатки збирають ваші особисті дані: Apple відкриє таємницю

Apple вимагає, щоб всі нові програми та оновлення програм дотримувалися політики конфіденційності розробників в App Store. Раніше всі програми на основі передплати повинні були посилатися на політику конфіденційності в своїх списках в App Store, але тепер це правило застосовується до всіх програм (Politeka).

Технічно Apple не вказала, що існуючі програми повинні слідувати новими правилами, тільки в майбутніх оновленнях має з'явитися посилання на політику конфіденційності. У ній говориться, що розробники повинні пояснити, які дані збирає їх додаток, і як його використовувати. Розробники повинні деталізувати свої зберігання даних і як користувачі можуть відмовитися і видалити свої особисті дані.

Правила вступають в силу 3 жовтня. Apple заявляє, що поточне програмне забезпечення без політики не буде видалено з App Store, але їм потрібно буде встановити посилання, якщо вони відправлять оновлення після цієї дати.

Після того, як 25 грудня GDPR був повністю введений в дію, а Facebook зазнали наслідки його серйозного фіаско порушення даних в березні, конфіденційність даних стала дуже важливою для технічних компаній. Це нове правило схоже на те, що Apple намагається відповідати більш високим очікуванням прозорості щодо того, як обробляються призначені для користувача дані, і просять розробників відрегулювати свої додатки.

***

5.09.2018

Уразливість у Android: хакери отримали повний доступ до будь-якого смартфону

У найсвіжіший версії Android 9.0 виявили критичну уразливість, внаслідок чого тепер зловмисники мають можливість отримати доступ важливої інформації на Вашому мобільному пристрої (Канал 24).

Відповідні результати дослідження оприлюднила американська компанія Nightwatch Cybersecurity, що займається дослідженнями в галузі кібербезпеки.

Як з'ясували фахівці, завдяки такому пролому у захисті хакери можуть отримати детальний доступ, зокрема, до інформації про Wi-Fi, назву підключення, включно з IP-адресою, DNS-сервера, паролю та інших параметрів.

Таким чином, зловмисники отримали можливість відстежувати увесь вхідний і східний трафік, перехоплюючи особисті дані

Крім того, знаючи детальну інформацію про смартфон, за допомогою шкідливого ПО можна відстежити будь-який смартфон і навіть влаштувати атаку на бездротову мережу та інші підключені до неї пристрої.

Додамо, що у Google уже знають про знайдену діру в безпеці Android, відтак компанія випустила «хотфікс» для Android 9.0. Щоправда, як підкреслює видання, патч закриває проблему тільки на 0,1 % всіх працюючих пристроях, інші ж 99,9 % моделей смартфонів перебувають у зоні високого ризику, і повністю захистити їх не видається можливим.

***

5.09.2018

Тысячи взломанных маршрутизаторов отправляют трафик хакерам

Исследователи безопасности из компании Qihoo 360Netlab сообщили об обнаружении новой вредоносной кампании, в ходе которой было инфицировано более 7,5 тыс. маршрутизаторов MikroTik по всему миру. Атака осуществлена с использованием уязвимости CVE-2018-14847 в компоненте управления Winbox, позволяющей удаленному злоумышленнику обойти аутентификацию и читать произвольные файлы. Проблема была исправлена производителем в апреле текущего года. По данным экспертов, в сети насчитывается порядка 370 тыс. маршрутизаторов MikroTik, уязвимых к атакам с использованием данной проблемы (InternetUA).

По словам исследователей, злоумышленники изменили настройки устройств таким образом, чтобы перенаправлять весь трафик на 9 принадлежащих им внешних IP-адресов.

«Самым используемым является адрес 37.1.207.114. Значительное количество устройств перенаправляет свой трафик именно на него», – отметили эксперты.

Как выяснилось в ходе анализа, злоумышленники проявляют усиленный интерес к портам 20, 21, 25, 110 и 144, которые предназначены для FTP, SMTP, POP3 и IMAP-трафика. Необычным является хищения трафика с портов SNMP (Simple Network Management Protocol) 161 и 162, которые, как правило, игнорируются в ходе подобных кампаний.

Наибольшее количество скомпрометированных устройств зафиксировано в России (1628), Иране (637), Бразилии (615), Индии (594) и Украине (544).

Данная атака направлена на заражение устройств с помощью скрипта для майнинга криптовалют Coinhive.

«Злоумышленники пытались майнить криптовалюту с помощью прокси-трафика с устройств пользователей», – отметили исследователи.

Однако, злоумышленники допустили ошибку и неправильно настроили списки контроля доступа к прокси, заблокировав таким образом все внешние web-ресурсы, в том числе необходимые для майнинга.

***

5.09.2018

В Google Play обнаружены сразу несколько банковских троянов

Четвертого сентября эксперт компании ESET Лукаш Стефанко (Lukas Stefanko) рассказал у себя в Twitter о трех банкерах, которые маскировались под астрологические приложения и насчитывали более 1500 установок.

Докладніше

***

5.09.2018

Правительственный сайт США допустил утечку данных граждан

Официальный сайт федерального правительства США foiaonline.gov, посвященный вопросам прозрачности и открытости правительственных действий, допустил утечку данных граждан. Ошибка во время обновления системы привела к раскрытию десятков, а то и сотен номеров социального страхования и другой персональной информации пользователей (InternetUA).

Проблема, затрагивавшая портал для подачи заявок на получение информации согласно закону «О свободе информации», была исправлена после того, как журналисты CNN сообщили о ней правительству. До исправления ошибки персональные сведения находились в открытой базе данных в течение нескольких недель, о чем не знали ни власти, ни пользователи.

Получив «наводку» от обнаружившего проблему источника, журналистам CNN удалось увидеть 80 номеров соцстрахования (полностью или частично), а также даты рождения, иммиграционные идентификационные номера, адреса проживания и контактные данные. Кроме того, в открытом доступе находились другие конфиденциальные сведения о пользователях. В одном случае жертва преступления запрашивала информацию о заведенном деле. Еще в ряде случаев утекли номера соцстрахования жертв кражи личности, запрашивавших данные по своему делу.

Проблема была связана с функцией поиска уже существующих запросов на раскрытие информации. Любой желающий мог увидеть, какие запросы уже были поданы и кем, а в некоторых случаях также предоставленные ответы на запросы. Эти описания были полностью видны на странице результатов поиска, в том числе номера соцстрахования и другие персональные данные. До обновления сайта с версии 2.0 до 3.0 в июле 2018 года персональные данные не отображались, однако после обновления вдруг стали видны.

***

6.09.2018

Популярное расширение для браузера Chrome похищает пароли пользователей

Исследователь безопасности под псевдонимом SerHack обнаружил в расширении MEGA.nz для браузера Google Chrome вредоносный код, позволяющий злоумышленникам похищать пароли от учетных записей Google, Amazon, Microsoft и GitHub, а также приватные ключи кошельков для криптовалюты Monero и Ethereum (InternetUA).

Вредоносный функционал был обнаружен в исходном коде расширения MEGA.nz версии 3.39.4. Инженеры Google уже вмешались и удалили расширение из официального интернет-магазина Chrome, а также отключили расширение для существующих пользователей.

Согласно анализу источника расширения, вредоносный код запускается на таких сайтах, как Amazon, Google, Microsoft, GitHub, MyEtherWallet и MyMonero, а также платформе для обмена криптовалютами IDEX.

Вредоносный код похищает имена пользователей, пароли и другие данные сеанса, необходимые злоумышленнику для авторизации. Расширение отправляет всю собранную информацию на сервер megaopac[.]host, размещенный в Украине.

Пользователям Chrome, использовавшим расширение, рекомендуется просмотреть раздел «Расширения» браузера и убедиться, что MEGA.nz отключено, а также сменить пароли и переместить криптовалюту на новые кошельки.

***

6.09.2018

Официальное приложение для iPhone обманом списывало $100 в неделю

Мошенническое приложение Ancestry, которое маскировалось под реальную компанию с таким же названием, обманом заставляло пользователей покупать премиум-версию, эксплуатируя механизм подтверждения платежей с помощью отпечатка пальца на устройствах Apple. Приложение распространялось через официальный AppStore.

Докладніше

***

6.09.2018

Сайт Донецкой ОГА оставил лазейку для российских хакеров

Владимир Кондрашов

«Дыра», через которую ранее российские хакеры взломали сайт Донецкой областной военно-цивильной администрации, спустя несколько месяцев вновь оказалась на портале (InternetUA).

Об этом на своей странице в Facebook сообщил спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд, передает InternetUA.

По словам хактивиста, уязвимость позволяет просмотреть любой файл на сервере, в том числе узнать root-пароль от MySQL.

Напомним, весной этого года российские хакеры взломали ресурсы Донецкой областной военно-цивильной администрации.

– Там был установлен web-shell, в логах – видна активность из Самары. Хакеры пытались зайти дальше в сеть. В таком виде Донецкая ОВЦА простояла недели две. Как мне потом объяснили люди, имеющие отношение к этой системе, они там устроили засаду. То есть, ждали, пока российские хакеры туда вернутся, чтобы что-нибудь о них ещё узнать. А в это время практически любой желающих мог лазить по их дискам прямо из браузера без пароля. Оттуда сразу открывался доступ во внутреннюю сеть, – рассказывал о ситуации спикер УКА во время конференции NoNameCon.

Тогда, спустя некоторое время портал всё-таки оказался вне доступа, ссылаясь «на технические неполадки», а потом вновь заработал как ни в чем не бывало. Но, как оказалось, уязвимость, использованная российскими хакерами, также оказалась на месте.

– Потом всё-таки сайт повалили, сослались на «временные технические неполадки» и сетью занялось ГП «Украинские Специальные Системы». И теперь дыра, через которую был взломан сайт, снова на месте. Я полагаю, что её восстановили из бэкапа. Она позволяет просмотреть любой файл на сервере, например, рутовый пароль от MySQL. Это всё, что вам нужно знать о CERT-UA, Госспецсвязи, ГП УСС и администраторах этой чудо-городушки, – прокомментировал спикер УКА.

***

6.09.2018
На сайте Генпрокуратуры обнаружили XSS-уязвимость
Владимир Кондрашов

«Не очень критическую, но неприятную» уязвимость обнаружил на сайте Генеральной прокуратуры Украины спикер Украинского Киберальянса, известный под ником Шон Таунсенд (InternetUA).

XSS – тип уязвимости программного обеспечения, который позволяет атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями.

– А вот в Генеральной прокуратуре Украины сидят умники. Вместо того, чтобы правильно экранировать запросы, кто-то решил повыёживаться и проверить, не содержит ли запрос «недопустимые символы», но проверяет только первый. То, что вы видите на экране, называется XSS-уязвимость, не очень критичная, но неприятная. Передайте кто-нибудь прокурорским, чтобы починили, – написал спикер УКА.

Напомним, со второй половины 2017-года украинские хактивисты проводят акцию #fuckresponsibledisclosure, направленную на поиск и публичное раскрытие уязвимостей государственных информационных ресурсов с целью

общественного влияния на уровень их безопасности. Около недели назад обнаружена XSS-уязвимость на сайте Государственного реестра избирателей ЦИК Украины, однако вместо благодарности ЦИК «наехала» на УКА.

За время проведения #frd хактивисты обнаружили и публично сообщили о нескольких десятках уязвимостей в информационных ресурсах и сетях государственных учреждений – в список попали Нацполиция, Энергоатом, CERT-UA, Пенсионный фонд и много других организаций.

***

6.09.2018

У США придумали суворе покарання за кіберзлочини // Президента зобов'яжуть складати список небезпечних в кіберпросторі діячів, а після вводити проти них санкції

У Сполучених Штатах Америки прийняли законопроект, який дозволяє накладати санкції на виконавців та замовників кібернетичних атак. Як передає НАРОДНА ПРАВДА з посиланням на Укрінформ, у Дональда Трампа вважають, що закон підтриманий обома партіями, захистить економіку країни (Народна правда).

Як пояснив голова Комітету Палати представників США Ед Ройс, законопроект вимагає,щоб президент формував списки небезпечних в кіберпросторі діячів – діячів, чиї дії становлять загрозу для національної безпеки, закордонних справ, економічного здоров'я або фінансової стабільності США.

Далі на тих, хто є в цьому «чорному списку», будуть накладати санкції.

***

6.09.2018

У Chrome знайшли баг, який робить «дірявими» мережі Wi-Fi

Для успішного проведення атаки необхідно зробити один клік. Вразливість стосується усіх заснованих на Chromium браузерів, таких як Google Chrome, Opera, Slimjet, Torch та інших.

Докладніше

***

7.09.2018

Twitter исследует возможности блокчейна для борьбы с мошенничеством

Глава Twitter и платежного стартапа Square Джек Дорси на слушаниях в Конгрессе 5 сентября заявил, что его компания исследует возможности применения технологии блокчейн для борьбы с мошенниками. Об этом сообщает CoinDesk (InternetUA).

«Вы ранее выразили интерес в широком применении технологии блокчейн, включая возможность идентификации личности для борьбы с недостоверной информацией и мошенниками. Какие возможные применения блокчейна вы видите?» – спросила представитель Калифорнии Дорис Матсуи на заседании Комитета по энергетике и торговле.

Глава Twitter отметил, что блокчейн отлично подходит для установления доверенных отношений в цифровом мире. Это особенно важно в свете заполонивших соцсеть поддельных аккаунтов, пытающихся обмануть пользователей и выманить у них криптовалюту.

«Первым делом надо начать с изучения проблем, которые нам надо решить и которые мы решаем, а затем посмотреть на доступные технологии и понять, какие из них помогут нам улучшить результат. Блокчейн, я думаю, та технология, которая имеет огромный и неиспользованный потенциал, особенно в областях распределенного доверия и, потенциально, распределенного правоприменения. Мы еще не достигли нужного уровня понимания, как могли бы применить эту технологию к проблемам, с которыми сталкивается Twitter. Но у нас есть люди, которые изучают этот вопрос», – ответил Джек Дорси.

***

10.09.2018

Британия обвинила российскую разведку в атаках на электросети

Великобритания обвинила Главное управление Генерального штаба Вооруженных сил РФ в осуществлении ряда кибератак на объекты своей критической инфраструктуры. Как рассказал журналистам The Daily Telegraph источник в британском правительстве, под киберудар попали энергетические сети, системы связи и СМИ (InternetUA).

Обеспокоенность по поводу роста числа кибератак на страну со стороны РФ глава Центра национальной кибербезопасности Великобритании (National Cyber Security Centre, NCSC) Киаран Мартин (Ciaran Martin) выражал еще в прошлом году. В частности об атаках на энергетические сети, телекоммуникационные и медиакомпании Мартин сообщил на саммите Times Tech Summit, проходившем в Лондоне почти год назад.

NCSC был основан в 2016 году, и за год своего существования предотвратил более 600 серьезных инцидентов. Связанные с правительством РФ группировки тестировали безопасность объектов британской критической инфраструктуры с целью выявления ее слабых мест, уверены в NCSC. Несмотря на то, что попытки злоумышленников получить полный доступ к атакуемым сетям не увенчались успехом, они могли собрать достаточно информации для подготовки более существенных кибератак.

***

10.09.2018

Ирина Фоменко

Популярнейшее приложение на Mac работает как шпионское ПО

Приложение для проверки безопасности Adware Doctor в настоящее время занимает четвертое место в списке популярных приложений для Mac App Store. Но после появления видеоролика Privacy 1st с доказательством подозрительной работы программы, исследователи безопасности Мас Патрик Уордл из Digita Security и Томас Рид из Malwarebytes проанализировали ее.

Докладніше

***

10.09.2018

Популярный браузер для любителей анонимности вышел на Android

Разработчики одного из самых популярных браузеров для анонимного выхода в интернет Tor объявили о выпуске официальной мобильной версии. Благодаря приложению никто не узнает о ваших поисковых запросах, используемом IP-адресе, скачанных файлах. Кроме того, Tor предоставляет доступ к заблокированным провайдером ресурсам (IGate).

Особенность Tor Browser заключается в применении так называемой луковой маршрутизации – системы прокси-серверов для установки анонимного подключения. Вместо прямого подключения к сайту Tor перенаправляет IP через несколько узлов после многоуровневого шифрования. Подобное решение стоит использовать в том случае, если вы обеспокоены проблемой анонимности в сети или вам нужен доступ к заблокированным сайтам.

***

11.09.2018

Доля атакованных компьютеров АСУ в первом полугодии в мире выросла до 41,2 %

«Лаборатория Касперского» опубликовала результаты исследований ландшафта угроз для систем промышленной автоматизации, полученные в течение первого полугодия 2018 г (Компьютерное Обозрение).

Доля атакованных компьютеров АСУ в первом полугодии в мире выросла на 3,5 % и составила 41,2 %. За год этот показатель увеличился на 4,6 %.

Сравнение показателей различных регионов мира показывает, что:

- страны Африки, Азии и Латинской Америки являются гораздо менее благополучными по проценту атакованных компьютеров АСУ, чем страны Европы, Северной Америки и Австралии;
- показатели Восточной Европы заметно выше, чем Западной;
- процент атакованных компьютеров АСУ в Южной Европе выше, чем в Северной и Западной Европе.

Можно предположить, что такая ситуация связана с объемами средств, вкладываемых организациями в решения для защиты инфраструктуры.

Основные источники заражения компьютеров в технологической инфраструктуре организаций – Интернет, съемные носители и электронная почта. Несмотря на расхожее мнение об изолированности технологической сети, именно Интернет за последние годы стал основным источником заражения компьютеров технологической инфраструктуры организаций.

В первом полугодии Интернет стал источником угроз, заблокированных на 27,3 % компьютеров АСУ, что на 6,7 % больше показателя первого полугодия 2017 г.

***

11.09.2018

США намерены вводить санкции против уличенных в кибершпионаже китайских компаний

Администрация президента Дональда Трампа рассматривает возможность ведения санкций в отношении китайских компаний, уличенных в краже интеллектуальной собстсвенности путем кибератак. Об этом сообщило агентство Bloomberg со ссылкой на осведомленные источники (InternetUA).

Американские власти намерены воспользоваться исполнительным указом, подписанным бывшим президентом страны Бараком Обамой. Документ разрешает США вводить ограничительные меры в отношении лиц или компаний, «вовлеченных в киберпреступную деятельность». Если администрация решит претворить в жизнь данную инициативу, США смогут изымать или замораживать находящиеся на территории страны активы уличенных в кибершпионаже китайских компаний, а также запретить им вести бизнес с американскими предприятиями.

Как отмечает агентство, не все члены текущей администрации согласны с необходимостью введения столь жестких мер. В частности, противником идеи является министр финансов США Стивен Мнучин, обладающий юрисдикцией в отношении потенциальных санкций.

На минувшей неделе Палата представителей Конгресса приняла законопроект, обязывающий президента страны вводить санкции в отношении лиц, организаций и государств, осуществлявших киберпреступления против США. По мнению членов парламента США, закон «О киберсдерживании и реагировании» позволит защитить инфраструктуру страны от «спонсируемой иностранными государствами вредоносной киберактивности» и подготовить базу для сдерживания и реагирования на подобные инциденты.

***

11.09.2018

Найдена опасная уязвимость в Windows

Антивирусная компания Eset обнаружила до сих пор не закрытую уязвимость в операционных системах Windows. Ее использует хакерская группировка PowerPool в целевых атаках в России, Украине, Польше, Германии, Великобритании, США, Индии, Чили и на Филиппинах (InternetUA).

Уязвимость представляет собой локальное повышение привилегий (Local Privilege Escalation), которое позволит выполнять вредоносный код с максимальными правами. Баг связан с работой планировщика задач Windows и затрагивает версии операционной системы Microsoft Windows с 7 версии по Windows 10.

Кибератака, использующая эту уязвимость, начинается с рассылки вредоносных спам-писем с бэкдором первого этапа. Внедряемый вирус предназначен для базовой разведки в системе – она выполняет команды атакующих и передает собранные данные на удаленный сервер.

Если компьютер заинтересовал хакеров, на нем будет установлен бэкдор второго этапа, обеспечивающий постоянный доступ к системе. Далее в PowerPool использует уязвимость нулевого дня для повышения привилегий. Для перемещения внутри скомпрометированной сети атакующие используют инструменты с открытым исходным кодом: PowerDump, PowerSploit, SMBExec, Quarks PwDump, FireMaster.

Атаки PowerPool нацелены на ограниченное число пользователей. Тем не менее, инцидент показывает, что злоумышленники отслеживают тренды и оперативно внедряют новые эксплойты. Раскрытие информации об уязвимостях до выхода обновлений безопасности может послужить причиной массовых кибератак, отмечают в Eset.

***

11.09.2018

Стало известно, как хакеры взломали сайт British Airways

Эксперты компании по борьбе с киберугрозами Risk IQ провели анализ атаки на авиакомпанию British Airways и обнаружили вредоносные строки в программном коде сайта, с помощью которых хакеры смогли получить информацию о личных данных сотен тысяч ее клиентов. Об этом говорится в докладе, опубликованном 11 сентября на сайте Risk IQ (Капитал).

По данным Risk IQ, злоумышленники использовали схему скимминга (кража данных карты при помощи считывающего устройства – Ред.) Magecart, но адаптировали ее к архитектуре интернет-страницы авиаперевозчика. «Этот скиммер очень хорошо приспособлен к организации платежей на сайте British Airways, что говорит о том, что исполнители очень дотошно продумали, как атаковать данный сайт вместо того, чтобы слепо внедрить скиммер Magecart», – считает эксперт компании.

Отмечается, что злоумышленники построили схему взлома так, чтобы она перемежалась с обработкой платежей, и это затрудняло ее обнаружение. Также

у экспертов есть подозрения, что доступ к сайту у хакеров появился еще до начала кибератаки, продолжавшейся с 21 августа по 5 сентября.

Шестого сентября British Airways заявила, что данные кредитных карт 380 тыс. клиентов авиакомпании оказались доступны злоумышленникам. Их жертвами могли оказаться все, кто бронировал билеты, оплачивал иные услуги на сайте или через приложение авиаперевозчика в период с 21 августа по 5 сентября. Клиентам компании, которые могли стать жертвами мошенников, рекомендовано обратиться в банк или другую кредитную организацию, выпустившую их карты, и следовать рекомендациям сотрудников службы поддержки. Руководство авиакомпании также обещает выплатить компенсации пострадавшим.

Как сообщило 7 сентября агентство Press Association, компании грозит штраф в размере до £500 млн (около $650 млн).

***

11.09.2018

Хакеры PowerPool используют в целевых атаках уязвимость нулевого дня

ESET предупреждает о целевых атаках с использованием новой, пока не закрытой производителем уязвимости в Microsoft Windows. По данным телеметрии, атаки нацелены на пользователей в России, Украине, Польше, Германии, Великобритании, США, Индии, Чили и на Филиппинах.

Докладніше

***

12.09.2018

Слежка за пользователями недешево обойдется компании Google

Штат Аризона расследует жалобы на слежку Google за своими пользователями (Телекритика).

Как сообщает издание The Washington Post, речь идет о неотключаемой функции контроля за местоположением пользователей мобильных приложений Google (например, «Карты» и «Поиск»).

Ранее стало известно, что если пользователь iOS- или Android-устройства не дает на это разрешения, многие сервисы Google все равно будут следить за ним, даже в том случае, если «история местоположения» умышленно отключена. Фактически ее отключение лишь означает, что информация не вносится в хронику действий и не видна пользователю.

Компания ранее отреагировала на обвинения, заметив, что делает это ради стабильной работы сервисов. Прокуратура Аризоны отказалась сообщать, сколько пользователей пожаловалось на Google. Если вина корпорации будет доказана, то штраф составит около 10 000 долларов за каждого истца.

***

12.09.2018

Опубликован эксплоит для критической уязвимости в Tor

Компания Zerodium, специализирующаяся на покупке и перепродаже эксплоитов, опубликовала в Twitter сообщение, в котором раскрыла информацию о критической уязвимости, затрагивающей браузер Tor. Брокер также обнародовал PoC-код для эксплуатации уязвимости (InternetUA).

Хотя компания описала проблему как уязвимость в Tor, в действительности она содержится в NoScript – популярном расширении для Firefox, предназначенном для защиты от вредоносных скриптов. Поскольку Tor разработан на базе Firefox, расширение входит в его состав по умолчанию.

Разработчик NoScript Джорджио Маоне (Giorgio Maone) устранил уязвимость спустя пару часов после публикации твита и выпустил новую версию расширения 5.1.8.7. По его словам, проблема существовала с мая 2017 года, когда вышла версия NoScript 5.0.4.

Как пояснил гендиректор Zerodium Чауки Бекрар (Chaouki Bekrar), эксплоит фактически обходит защиту NoScript, даже если в Tor установлен наивысший уровень безопасности.

«Если пользователь установит уровень как «Наиболее безопасный» для блокировки JavaScript-кодов со всех сайтов (т.е. предотвращения внедрения браузерных эксплоитов и сбора данных) эксплоит позволит сайту или скрытому сервису обойти все ограничения NoScript и выполнить любой код JavaScript, несмотря на максимальный уровень защиты», – рассказал Бекрар.

По его словам, компания приобрела эксплоит «много месяцев назад» и уже успела поделиться им с правительственными структурами, которые, предположительно, использовали его для «борьбы с перступлениями и насилием над детьми». Бекрар также отметил, что уязвимость не затрагивает версию Tor 8 и порекомендовал пользователям обновиться до новой редакции браузера.

***

13.09.2018

У Євросоюзі схвалили нові вимоги до авторського права в Інтернеті // Рекламні гіперпосилання тепер можуть підлягати оподаткуванню

Європарламент ухвалив з поправками директиву про авторське право в Інтернеті. Документ спершу був відхилений, але в підсумку набрав необхідну кількість голосів (ТСН).

Критикам документу особливо не подобалися 11-та та 13-та статті, що присвячувалися встановленню оподаткування посилань і відповідальності онлайн-платформ за контент своїх користувачів. Підсумкова редакція документу містить положення про те, що невеликі платформи будуть звільнені

від сплати податку, а сам він не поширюватиметься на «просту публікацію гіперпосилань». Також від оподаткування звільнені проекти типу Wikipedia.

Також депутати Європарламенту відкинули ідею зобов'язати платформи автоматично видаляти контент, що порушує авторське право. Натомість компанії мають забезпечити вільне завантаження інформації, що не містить порушень вимог щодо авторських прав.

***

14.09.2018

Каждая четвертая кибератака нацелена на частных лиц

По данным Positive Technologies за II квартал, количество инцидентов кибербезопасности выросло на 47 % по сравнению с прошлогодним. При этом доля целевых атак превысила долю массовых и составила 54 %.

Докладніше

***

15.09.2018

Хакеры атаковали личные аккаунты журналистов «1+1 media»

С началом телевизионного сезона и выходом новых выпусков программы «Гроші», участились случаи попыток вмешательства в работу сотрудников Департамента журналистских проектов «1+1 media» посторонними лицами. Так, ночью с 14 на 15 сентября на журналистов канала совершили целенаправленную и массированную хакерскую атаку (Телекритика).

Злоумышленники пытались получить доступ к телефонам, мессенджерам и личным страницам в соцсетях представителей департамента журналистских расследований, в частности, ведущего программы «Гроші» Александра Дубинского и руководителя Департамента журналистских проектов Максима Шиленка и других журналистов.

Учитывая характер действий злоумышленников, а также беря во внимание, что случаи вмешательства в работу украинских журналистов с началом предвыборной конкуренции становятся все более частыми, телеканал расценивает это как реакцию на расследование о деятельности чиновников высокого ранга.

Попытки взлома были зафиксированы и предупреждены службой безопасности канала. В дальнейшем компания еще больше усилит все необходимые меры безопасности для защиты информации сотрудников.

***

16.09.2018

Хакеры украли миллионы документов из престижных вузов Британии

Иранские хакеры похитили миллионы документов из наиболее престижных университетов Великобритании. Об этом сообщает The Daily Telegraph (InternetUA).

По данным издания, хакеры похитили документы связанные с кибербезопасностью и атомными электростанциями.

Как отмечается, документы были выставлены на продажу на нескольких сайтах на фарси.

При этом, в частности, хакеры похитили материалы из Кембриджа и Оксфорда.

***

16.09.2018
Как посты в соцсетях могут помешать получить кредит

Банки, страховые компании и продавцы техники уже давно используют так называемый скоринг по соцсетям, чтобы принять решение об одобрении кредита человеку или об осуществлении для него других операций. Людей просто проверяют.

Докладніше

***

17.09.2018
Как понять, что вашу переписку кто-то читает

Использует ли кто-то посторонний ваши аккаунты? Почти во всех сервисах это можно проверить за пару кликов.

Докладніше

***

17.09.2018
Владимир Кондрашов
Украинская наука не дружит с кибербезопасностью

В рамках акции #fuckresponsibledisclosure Украинский кибералъянс обнаружил множественные уязвимости на порталах целого ряда высших учебных заведений и научных учреждений страны (InternetUA).

Сведения об уязвимостях двадцати одного портала опубликовал у себя на странице в Facebook спикер Украинского кибералъянса, известный под ником Шон Таунсенд.

Украинский кибералъянс обнаружил проблемы с безопасностью на порталах Запорожского национального университета, Украинского государственного университета железнодорожного транспорта, Национальной библиотеки имени Вернадского, Полтавского национального университета имени Короленко, Полтавского национального технического университета

имени Кондратюка, Учебно-научного института экологической безопасности Национального авиационного университета, Черноморского национального университета имени Петра Могилы, Киевского Университета имени Бориса Гринченко, Института информационных технологий Ивано-Франковского национального технического университета нефти и газа, Одесской юридической академии, Тернопольского национального педагогического университета имени Гнатюка, Национального института пищевых технологий, Военного института танковых войск ХПИ и Львовского национального университета имени Франко.

Кроме научных учреждений, в списке также сайт институций гражданского общества Винницкого горсовета, Свялявская РГА, Совет предпринимателей тернопольской области, Свято-Успенская Почаевская лавра, Николаевводоканал, Запорожское отделение Укргосфонда поддержки фермерских хозяйств и даже Киевский международный институт социологии. Если многие администраторы и руководители учреждений поблагодарили УКА за выявление брешей в защите, то в последнем случае КМИС отреагировали не совсем адекватно.

Как стало известно, в большинстве случаев на данных порталах обнаружены SQL и XSS-уязвимости. Некоторые сайты уже оказались взломаны иностранными хакерами, при чем – довольно давно.

***

17.09.2018

На ресурси Вселенського патріархату здійснюють потужні кібератаки, - Клімкін

На тлі призначення Константинополем повірених у Києві на ресурси Вселенського патріархату почали здійснювати масовані кібератаки

Про це повідомив у Facebook міністр закордонних справ України Павло Клімкін (Espreso.tv).

«Багато вражень та емоцій після першої зустрічі з екзархами його Всесвятості Вселенського Патріарха. Однак, про одну річ хочу сказати вже зараз. Останнім часом і на Фанар, і на Вселенський патріархат, і на самих екзархів відбуваються масовані кібератаки», – написав глава МЗС.

***

17.09.2018

Microsoft встроила защиту от вирусов в макросах в приложения Office 365

На этой неделе Microsoft сообщила об интеграции системы Antimalware Scan Interface (AMSI) в клиентские приложения Office 365. AMSI берет на себя ответственность за поиск и обнаружение вредоносных макросов и скриптов

внутри офисных документов, предотвращая таким образом их исполнение и нанесение вреда вашему компьютеру (InternetUA).

Вирусы на основе макросов всегда были популярной «входящей точкой» для вредоносного ПО и на протяжении последних лет мы видим их стремительное возрождение. Постоянные улучшения платформы и систем безопасности позволили уменьшить количество софтверных эксплойтов, но злоумышленники нашли альтернативные способы внедрять зараженный код путем использования VBA-макросов.

В дополнение к внедрению систем AMSI в офисные приложения, Microsoft сообщила, что разработчики сторонних антивирусов смогут использовать открытый интерфейс AMSI в своих решениях. При обнаружении подозрительного поведения AMSI будет мгновенно останавливать работу макроса и уведомлять пользователя через интерфейс Office. После этого работа приложения будет останавливаться полностью для предотвращения дальнейшего вреда.

AMSI уже доступна для подписчиков Office 365 в приложениях Word, Excel, PowerPoint, Access, Visio и Publisher.

***

18.09.2018

Проти Держдепартаменту США влаштували кібератаку: вдалося вкрасти деякі дані

Державний департамент США нещодавно зазнав хакерської атаки проти своєї некласифікованої системи електронної пошти, в результаті чого було викрито дані невеликої кількості співробітників (Espreso.tv).

У Держдепі описали цей інцидент як «діяльність, що викликає заклопотаність, яка вплинула менш ніж на 1 % поштових скриньок співробітників».

Представники відомства визнали, що персональні дані деяких співробітників могли бути викриті, та повідомили їх про це.

Відповідно до попередження, класифікована система електронної пошти не була зламана.

Держдепартаменту неодноразово вказували на його недостатню захищенність у питанні кібербезпеки, зокрема минулого тижня сенатори зажадали звітності від держсекретаря Майка Помпео щодо цього. Останній досі не відповів на лист сенаторів.

Один зі співрозмовників видання розповів, що після зламу електронної пошти Департамент скликав цільову групу для розслідування інциденту. Наразі у відомстві не говорять, хто саме може бути причетним до кібератаки.

ДОДАТКИ

Додаток 1

4.09.2018

WhatsApp лишился поддержки iPhone 4 и стал безопаснее

Разработчики WhatsApp представили обновленную версию фирменного мессенджера для платформы iOS, которая уже доступна для загрузки в App Store. Несмотря на то, что многие пользователи могут даже не заметить выхода апдейта, установить его смогут только владельцы устройств, работающих под управлением iOS 8 и новее (Portaltele).

Поскольку ранее разработчики WhatsApp обещали обеспечить поддержку iPhone с iOS 7 до 2020 года, их владельцы по-прежнему смогут пользоваться предыдущей версией мессенджера.

Однако, если они захотят испытать нововведения актуальной версии, им придется обновить ревизию iOS до более свежей, чего не смогут сделать владельцы iPhone 4.

Подозрительные ссылки

Одним из наиболее значимых нововведений последнего апдейта WhatsApp, помимо прекращения поддержки iOS 7, является усовершенствованная система безопасности, предупреждающая о подозрительных ссылках.

Например, если кто-то пришлет вам ссылку, которая ведет на мошеннический веб-ресурс, WhatsApp предупредит вас об этом. Поскольку WhatsApp не проверяет сами ссылки, не исключена вероятность ошибки.

Это связано с тем, что мессенджер всего лишь локально анализирует комбинации символов, из которых состоит адрес сайта. Так он обнаруживает повторы букв в доменных именах и перестановку их местами, чем пользуются мошенники, выдавая поддельный сайт за настоящий.

Предпросмотр вложений в уведомлениях

Кроме того, у пользователей обновленного WhatsApp для iOS появилась возможность просматривать, какие медиавложения содержат входящие сообщения, не открывая самих посланий.

Данная функция доступна только владельцам устройств под управлением iOS 10 и новее из-за особенностей работы системы уведомлений.

(вгору)

Додаток 2

6.09.2018

Йдемо. Понад чверть американців запевняють, що відмовилися від додатку Facebook // Користувачі кажуть, що залишають Facebook

Понад чверть користувачів Facebook із США кажуть, що вони видалили додаток соцмережі зі своїх телефонів за останній рік (Новое время).

Це відбувається як свого роду реакція на проблеми соцмережі із забезпеченням конфіденційності користувачів, пише Recode.

Крім того, згідно з опитуванням, проведеним дослідницьким центром Pew, 42 % американців кажуть, що вони зробили перерву у використанні Facebook протягом декількох тижнів або більше. Ще 54 % відсотка запевняють, що вони коректували настройки конфіденційності протягом минулого року.

Молодші користувачі Facebook частіше згадують, що вони видалили додаток: близько 44 % опитаних у віці від 18 до 29 років кажуть, що вони видалили додаток Facebook за останній рік, проти 12 % користувачів у віці 65 років і старше.

Цікаво, що, судячи з усього, це не суттєво вплинуло на розмір аудиторії Facebook. Щоденна активна призначена для користувача база Facebook в США та Канаді залишається приблизно на рівні 185 млн користувачів протягом чотирьох кварталів поспіль. Можливо, користувачі видаляють додаток, а потім встановлюють його заново. Також можливий варіант, що люди почали користуватися Facebook через веб-версію, відмовившись тільки від програми, а не від самої соцмережі.

З квітня по червень 2018-го, кількість щоденних активних користувачів Facebook зросла у США та Канаді всього лише на 1 % порівняно з минулим роком. А саме ці регіони приносили для соцмережі основний прибуток від реклами.

При цьому виручка Facebook у другому кварталі 2018 року підскочила на 42 % і досягла $13,2 млрд. Аналітики в середньому оцінювали виручку Facebook майже в $13,4 млрд. Останній раз виручка компанії виявлялася гірша прогнозу в першому кварталі 2015 року.

(вгору)

Додаток 3

12.09.2018 126

В мобильном приложении YouTube появилась новая функция // YouTube добавил счетчик времени просмотренных видео

На конференции разработчиков Google I/O 2018 компания анонсировала появление ряда инструментов, направленных на то, чтобы пользователи сервисов лучше понимали, на что конкретно они тратят время. Данная информация может помочь сфокусироваться на том, что приносит пользу и отказаться от того, что не мешает развитию. Начиная с 12 сентября подобные инструменты появились в видеосервисе YouTube, благодаря чему каждый любитель видеоблогов теперь может точно узнать, сколько времени у него уходит на просмотр свежих выпусков любимых авторов (seMobile).

Для того, чтобы функция подсчета времени работала, в YouTube-аккаунте должна быть включена функция записи истории просмотра видео. Нажав на иконку профиля, вы получите доступ к меню «Ваше время просмотра», где собрана информация о том, сколько именно вы смотрели видео сегодня, вчера и

за последнюю неделю. В том же меню подсчитывается среднее ежедневное значения времени просмотра видео.

Если время просмотра видео неприятно вас удивило, ты вы можете установить напоминание (ползунок чуть ниже в том же меню «Ваше время просмотра»), которое будет всплывать через определенные промежутки времени, напоминая, что стоит прерваться и дать отдохнуть своему зрению и мозгу. По умолчанию предлагается промежуток 1 час 15 минут, однако в этом меню можно самостоятельно выбрать любой подходящий интервал с шагом 5 минут.

Активные пользователи YouTube, подписанные на несколько каналов, знакомы с ситуацией, когда уведомления о новых видео появляются чуть ли не каждый час. При этом далеко не все могут сразу приступить к просмотру, так как сидят на уроках или в офисе. Теперь YouTube предлагает возможность получать в удобное время одну регулярную сводку, в которой соберут все уведомления за целый день. Таким образом, пользователь сервиса получит сводку именно тогда (например, в 9 вечера), когда все запланированные дела сделаны и он может спокойно просмотреть все новинки.

И, наконец, можно выбрать «Тихие часы», во время которых звуковые сигналы и вибрация уведомлений будут автоматически отключены, чтобы не разбудить вас или членов вашей семьи, когда одному из авторов захотелось провести стрим или выложить новый ролик посреди ночи. По умолчанию тихие часы назначены на промежуток с 22:00 до 8:00, однако его также можно изменить самостоятельно.

Новые функции отслеживания времени на YouTube постепенно появятся у всех пользователей сервиса, вы можете проверить их наличие, нажав на иконку своего аккаунта в верхнем правом углу мобильного приложения.

(вгору)

Додаток 4

12.09.2018

Розроблений у Facebook штучний інтелект Rosetta допоможе соцмережі зрозуміти меми

Мемом може вважатися будь-яка ідея, символ, манера або образ дії, які свідомо чи несвідомо передаються від людини до людини за допомогою мови, листів, відео, ритуалів, жестів. Але користувачам інтернету меми більше відомі у вигляді картинок з написом на них (TechToday).

Активні інтернет-користувачі могли помітити, що останніми роками стало популярним спілкування за допомогою картинок з написами. І якщо для людини такий формат зручніший, ніж текст, з ним виникають складнощі в інтернет-гігантів. Найбільша соцмережа планети Facebook адаптувала свою систему штучного інтелекту Rosetta, яка вже займається перекладами та пошуком хейтерських фраз, для розпізнавання тексту на зображенні.

Мем (англ. Meme) – одиниця культурної інформації. Мемом може вважатися будь-яка ідея, символ, манера або образ дії, які свідомо чи несвідомо передаються від людини до людини за допомогою мови, листів, відео, ритуалів, жестів. Але користувачам інтернету меми більше відомі у вигляді картинок з написом на них. Подібний спосіб пересилання інформації став настільки популярним, що меми також часто називають медіавірусами, оскільки найбільш вдалі поширюються в соцмережах та на сайтах вибуховим чином. В інтернеті навіть є спеціалізовані онлайн-генератори мемів, з якими не потрібно вміти користуватися фоторедакторами, щоб нанести напис на завантажене на сайт зображення.

Розуміти меми необхідно, щоб їхній зміст став доступний іншомовним користувачам, а також переконатися в тому, що завантажений контент не розпалює ворожнечу чи якимось іншим чином порушує правила соцмережі. У Facebook кажуть, що Rosetta «витягує» текст з понад мільярда картинок та відеокадрів щодня. Причому слова написано різними мовами, з арабською та хінді включно.

Розробники системи говорять, що її широко використовують у Facebook та Instagram для аналізу завантаженого контенту. У планах – розширити кількість підтримуваних Rosetta мов для якіснішого аналізу тексту на картинках. Система нещодавно додала ще 24 мови, разом з телугу, непальською, урду, панджабі та зулу.

До речі, з точки зору юриста меми – це не просто картинки з написами, вони мають права. У 2013 році Grumpy Cat Limited уклала угоду з фірмою з випуску напоїв Grenade. Вони запустили бренд охолодженої кави Grumpy Cat Grumpuccino, в якому без дозволу використали популярний мем з невдоволеним котом. Три роки потому суд виніс вердикт, який може стати прецедентом для інших мемів.

А ще від сучасних мемів весело буде також археологам майбутнього. Представники популярного гумористичного інтернет-майданчика 9GAG висікли на 24-тонній кам’яній плиті меми. Після цього вони закопали її посеред пустелі в Іспанії. На носій потрапили персонаж DickButt, «замислений динозавр» філософаптор і стоп-кадр з кліпу Pen-Pineapple-Apple-Pen корейського музиканта Піко-Таро.

На Android можна легко перейти на спілкування мемами. Для цього знадобиться додаток Meme Generator, який розповсюджується безплатно, а за $2,49 позбавляє від вбудованої реклами. Відразу після його запуску він запропонує широкий вибір картинок із уже популярних мемів. Щоб знайти потрібну, необхідно лише ввести її назву в поле пошуку. А якщо натиснути на зірку поряд із зображенням, це зробить його «улюбленим». Окрім вбудованого набору картинок, можна використовувати свої власні фотографії. Щоб створити мем, необхідно вказати знімок, а також написати два рядки тексту вгорі та внизу. Після цього можна відразу переслати його друзям або зберегти на майбутнє.

(вгору)

Додаток 5

6.09.2018

Менше чверті депутатів Полтавської міськради комунікують з виборцями в соцмережі

Чинне законодавство України визначає, що депутат місцевої ради перш за все є представником громади та виборців, чиї інтереси він і зобов'язаний захищати. Звісно ж, для того, щоб знати, що саме виборювати і чого домагатися, депутат має комунікувати зі своїми виборцями. Задля цього, законодавство пропонує такі форми взаємодії: прийом виборців, зустрічі з ними, отримання наказів від виборців та звітування (Коло).

Нинішній розвиток технологій, зокрема інтернет-середовища, значно розширює можливості депутатів. Адже, маючи, для прикладу, сторінку в соціальній мережі можна взаємодіяти з людьми, оперативно дізнаватися про проблеми громади, не влаштовуючи спеціальних зустрічей. Звісно, реєструватися у соцмережах депутатів ніхто не зобов'язує, однак за грамотного підходу до ведення своєї публічної сторінки, можна не лише ефективно комунікувати з громадянами, а й підвищувати свій рейтинг серед населення.

Наразі наймасовішою в світі і законною в Україні соцмережею є Facebook. Тож, ми вирішили перевірити, чи користуються депутати Полтавської міської ради цією соціальною мережею, аби спілкуватися зі своїми виборцями.

Почнемо з того, що майже третина депутатів (11 осіб) взагалі не мають сторінок у цій соцмережі. Так, у Facebook виборцям не знайти більшість фракції «Совість України» (Ліліану Бєлашову, Максима Голдиша, Владислава Киву, Володимира Левченка, Григорія Сахна), трьох депутатів міськради від БПП «Солідарність» (Віталія Павлія, Володимира Печерицю, Вячеслава Федоряку), Дмитра Батигіна і Олександра Кудацького з «Рідного міста» та безпартійного Сергія Луценка.

Ще шестеро депутатів (16 %), хоч і зареєстровані у Facebook, проте гребують публікувати на своїх сторінках бодай якусь інформацію. Серед них: Олег Бєлоножко, Олександр Пінчук ВО «Батьківщина», Ірина Климко, Володимир Медяник «Совість України», Володимир Корчака БПП «Солідарність» та Тарас Синяговський ВО «Свобода».

Наступну когорту можна умовно назвати «невидимками» для виборців. Адже їхні сторінки у більшості випадків не відображають причетності власників до політичної діяльності. Серед депутатів, які використовують Facebook радше в особистих цілях, Андрій Соколов «Батьківщина», Юрій Бойко «Самопоміч», Юлія Мелкумова БПП «Солідарність» та Світлана Нестуля «Рідне місто».

Далі мова піде про депутатів, які хоч і створюють публікації суспільно-політичної тематики, проте не відповідають на коментарі дописувачів, або ж відписують лише на залишені під особистими фото чи публікаціями, не

пов’язаними з депутатською діяльністю. До цієї групи віднесемо Андрія Матковського, Олександра Глазова БПП «Солідарність», Олександра Кісільова «СДП», Анатолія Клименка, Дмитра Петрова «Батьківщина», Анатолія Костенка та Сергія Литвиненка «Свобода».

Взаємодіють з виборцями у Facebook менше чверті від складу депутатського корпусу Полтавської міськради (їхні прізвища розташуємо від нижчого рівня активності комунікації з громадянами до найвищого, враховуючи кількість публікацій-звітувань перед виборцями та спілкування з дописувачами). Тож, до «чудової» вісімки увійшли Майя Матвеєва БПП «Солідарність», Сергій Бутко «Самопоміч», Артем Чубенко «Свобода», Юрій Синяк «СДП», Вадим Ямщиков «Свобода», Дмитро Сенчакович «Самопоміч», Юліан Матвійчук «Свобода» та Олександр Шамота «СДП». Зазначимо, деякі депутати використовують на своїх сторінках у якості звітування відеоконтент (звернення до громадян, прямі ефіри), що покращує рівень сприймання виборців.

Окремо хочемо виділити публікації у Facebook з розряду «і депутати теж люди». До речі, у деяких членів корпусу такими дописами вдається краще підвищувати рейтинг свого профілю, ніж публікаціями, які стосуються депутатської діяльності.

Не мають сторінки у Facebook – 11 депутатів (30 %)

Мають сторінку, проте її не використовують – 6 (16 %)

Використовують сторінку радше в особистих цілях – 4 (12 %)

Не відповідають на коментарі до соц.-політ публікацій – 7 (20 %)

Спілкуються з виборцями – 8 (22 %).

(вгору)

Додаток 6

3.09.2018

Гра «Момо»: що це таке і що потрібно знати про нову смертельну гру для підлітків

Катерина Петренко

Нещодавно у мережі з’явилась моторошна розвага «Момо», що провокує самогубство дітей зі слабкою психікою, на кшталт суїцидальної гри «Синій кит». Імовірно, вона вже підбирається до України.

Що варто знати про цю страшну забавку, хто її розробник та чи зареєстровані у світі випадки самовбивств, спровоковані іграшкою – розбирались журналісти 24 каналу.

«Момо»: що це таке?

Жіночка з вирячениими очима, величезним ротом та курячими лапами неочікувано з’являється у списку ваших контактів у месенджері WhatsApp. Усі спроби видалити її, як правило, марні. Контакт з моторошною аватаркою з’являється знову і знову. Далі починає писати, що все про вас знає і що ви

помрете через кілька днів. А також легко переходить на мову співбесідника і спілкується простими фразами.

Потім погрожує, надсилає файли із сценами насилля, детальну інформацію про вас і дає вказівки до самознищення. Інколи ця жіночка телефонує, і лякає вас плачем, який переходить в істеричний сміх.

За словами віце-президента Української асоціації психоаналізу Володимира Мамко, «Момо» – не що інше, як прототип матері.

«Ця гра розрахована на певну категорію дітей, які залежні від думки інших. Вони хочуть відповідати чиїмось очікуванням, бути улюбленцями батьків. І якщо вони чують загрозу, що буде погано їхнім близьким, мамі, наприклад, то вони готові виконати всі вимоги», – зазначив Мамко.

Як «Момо» отримує детальну інформацію про «жертв»?

Вочевидь, це не демониця, а звичайнісінький бот.

Все просто. Доки ви переглядаєте надіслане «куратором» відео, програма зчитує персональні дані з смартфону. Підліток бачить неоприлюднені в мережі свої фото, відео, адреси й телефони, не відразу розуміє, що все це – з його ж телефону, тому лякається і починає вірити у справжню «демоницю» мережі.

Якщо в дитини серед цих даних є щось «гаряченьке», що вона хотіла б приховати, її можна шантажувати. А там і до спроб самовбивста недалеко…

Чи призводила забавка до самогубств?

Достеменно невідомо, адже гра з’явилась місяць тому. Однак, ЗМІ повідомляли, що суїцид 12-річної дівчинки в Аргентині 22 липня стався саме через «Момо». Тіло дівчинки висіло на мотузці, а поруч лежав телефон. «Зламавши» пароль, знайшли переписку з моторошним персонажем в месенджері WhatsApp, повідомляли в поліції. Чим закінчилось розслідування – наразі невідомо, останні новини про інцидент датовані 25 липня.

ЗМІ також посилались на заяви іспанських та американських правоохоронців, які в липні застерігали від контактів з користувачами, які на аватарці використовують зображення моторошної жіночки. Бо відеоролики про неї з’явились польською і німецькою мовами 26 липня.

Інформаційний вірус вже добрався до Росії. «Момо» з’явилась в російському сегменті інтернету теж в кінці липня – на початку серпня через ютуб-канали про відеогру Minecraft.

За тиждень російські відеоблогери записали кілька десятків відео, в яких телефонують за номерами, які, нібито, належать «кураторам», розказують страшні історії про «Момо» або роблять гумористичні скетчі. У деяких випадках переписуються в WhatsApp і отримують повідомлення на кшталт «Ти помреш». Хто за цим стоїть, невідомо.

Про засилля «Момо» в українському сегменті інтернету ще не йдеться.

Що відомо про розробників?

Цікаво, що зображення «Момо» – це фотографія скульптури японського художника Мідорі Хаясі, яка зображує птаха-матір. Вона з’явилась в музеї жахів у Японії ще в 2016-му році і, вочевидь, не має нічого спільного з моторошною забавкою, яка стрімко розповзається світом.

«Момо» вперше з'явилась у Facebook 30 червня. Хтось попросив у повідомленні про допомогу і вказав свій номер телефону. Інформація поширювалась швидко, і багато людей потрапляли на цей гачок і телефонували. Таким, чином, вважають спеціалісти, програма «Момо» поширювалась світом. Це якщо брати матеріальний бік подій. Але ж у світі є багато людей, які свято вірять, що «Момо» – це демониця, яка живе і владарює у мережі і в мобільних телефонах…

Як уберегтися?

Спробувати захистити смартфони своїх дітей від шкідливих впливів за допомогою спеціальних програм, або ж геть видалити меседжер WhatsApp. А краще – проводити більше часу зі своїми чадами, а не віддавати їх на поталу мережам.

(вгору)

Додаток 7

10.09.2018

Як Facebook спростив людське спілкування

Онлайн-сервіси потребують контенту, який можна легко класифікувати. Це вплинуло і на людей. Письменник та колишній інженер Microsoft та Google Девід Аувербах (David Auerbach) пояснив як інтернет змінює сучасне спілкування. Якщо у двох словах, то люди змушені реагувати на контент простими діями, що, у свою чергу, поєднує людей та сприяє спілкуванню (Blog.Imena.UA).

Простий рівень зворотного зв'язку між користувачами, який просувається онлайн сервісами – то скоріш фішка, а не помилка в системі. Комп'ютеру простіше обробити смайлик чи лайк, ніж сам текст. Відгуки користувачів потрібні людям для того, щоб оцінити якість послуг в ресторані, але додатки не існували б без рейтингів. Завдяки рейтингам тепер зручно сортувати, фільтрувати та проводити історичний аналіз закладів. Це приводить до…

Перший закон інтернет-даних

У будь-якому контексті структуровані дані насправді лежать на поверхні.

Структуровані дані – це будь-які дані, що несуть за собою категорії кількісного значення або рейтинги. Вони не потребують контексту для свого використання. Дані, що існують в структурованому вигляді, такі як транзакції, категорії продуктів в інтернет-магазинах або анкети в Facebook стануть більш корисними та знаковими для алгоритмів, людей та компаній, які їх використовують. Як приклад таких даних, можна навести текст, відео або ж зображення.

Жорстка структуризація стала розвиватися більше з появою соціальних платформ таких як Twitter, Facebook, Snapchat, Instagram. Також сюди можна віднести і торгові платформи типу Amazon та eBay.

Суть проекту Веб 2.0 лежить в соціальній взаємодії. Google заполонив ринок неструктурованих даних. З часом інтернет почав вимагати більш

ретельної структури контенту, який було б простіше аналізувати. А кращий спосіб зробити це в глобальному вимірі – це найняти користувачів, які створювали б такі дані.

Такі структуровані дані мають бути розмічені та класифіковані перед тим, як їх відсортують. Проекти архівів такі, як Бібліотека Конгресу, не сортують книги. Вони розробляють спеціальну класифікацію, яка визначає їх порядок. Нема класифікації – нема сортування.

Другий закон інтернет-даних

Для будь-якого кластеру даних, класифікація набагато важливіша за об'єкт, що класифікують.

Висновки та вплив аналізу отриманих даних витікають з класифікації, по якій вони збиралися, а не з самих даних. Коли Facebook за певним алгоритмом об'єднує людей по інтересах (любителі серіалів чи законодавці моди), нема певної риси, за якою людей в цій спільноті щось об'єднувало б. У класифікації Facebook немає нічого особливого. Це лише домішок особистих факторів, які у разі їх компонування, вони запускають певні категорії. Європейські люди, які виявили «спільну етнічність» з афроамериканцями були б дуже здивовані.

Важливо зазначити, що така категорія існує тому, що вона визначає як до людини будуть відноситись в майбутньому. Назва категорії, як би вона не називалася набагато важливіша, ніж критерій для неї. Критерії Facebook для категорій «афроамериканців» або «етнічна меншість» в основному будуть збігатися. В кожному випадку кінцева класифікація має зовсім різне значення. Але відмінність між критеріями класифікації досить розмита. Ми ніколи їх не бачимо. Вони зазвичай помилкові. Вибір класифікації набагато важливіший за процес самої класифікації.

Тут сам Facebook та інші класифікатори лише посилюють чинні проблеми таксономій. Уявлення про економіку залежить від визначеності безробітності (люди, що не шукають роботу, співробітники на неповний робочий день, тимчасові заробітки тощо), а не від досвіду та думок окремих жителів. Ваша думка про своє здоров'я залежить від того, чи класифікується ваша вага, дієта та спосіб життя як «здорові» або «нездорові», а не від наявної статистики. Навіть такі поняття, як «товстий», «людина з зайвою вагою» і «людина, що страждає від ожиріння» – асоціації, які визначають як «читається» така класифікація. Декотрі класифікації набагато вдаліші та популярніші за інші. Головне емпіричне правило…

Третій закон інтернет-даних

Прості класифікації будуть перемагати складні.

Механізм зворотного зв'язку (лайки, зірочки) насправді навмисний. Інтернет-сервіси можуть працювати зі складними онтологіями, якщо це потрібно, але все ж прості механізми є більш популярними. Facebook довелось чекати 10 років, щоби ввести інші реакції окрім «лайків». Вони не зважали на прохання ввести функцію «дизлайку». Тут з'явився дисонанс, коли люди ставили лайки напроти посту про смерть або ще якісь страшні злочини. Він віддавав перевагу простій бімодальній метриці «цікаво/нецікаво». Але коли все

ж керівництво соцмережі вирішило дослухатися до рекомендацій користувачів, вони добавили шість емоційних відгуків: «подобається», «супер», «співчуваю», «ха-ха», «обурений» та «ух ти!». Дві останні негативні емоції «співчуваю» та «обурений» виглядають визначнішими, ніж інші. Якщо людині подобається новина, вона ставить позитивну реакцію, це взиває певну взаємодію з її вподобаннями. Якщо ж людина обурена побаченим або злиться на пост, значить вона не бажає бачити подібне у своїй стрічці. В негативних реакціях Facebook не зацікавлений.

Шість реакцій схожі на емодзі, що дозволяє користувачам не набирати емодзі в коментарях, а швидко прореагувати на той чи інший запис. А ще вони виглядають простіше, ніж більшість смайликів у Facebook. Онлайн-сервіс Buzzfeed використовує схожу схему реакцій читачів на статтю. Вона спеціально розроблена для дослідження ринку, щоб відстежувати що для читачів шокуюче, миле, смішне і т. д.

Сара Фрайєр (Sarah Frier) з Bloomberg пояснила як Facebook створював нові смайлики.

З самого початку співробітники соцмережі зібрали найпопулярніші відповіді користувачів на пости, такі як «лол», «шок», «ахаха», «сміх» і т. д. Потім вони сформулювали шість відповідей: злий, сумний, вау, хаха, еее, та люблю. Реакцію «еее» довелося замінити, оскільки така реакція «не зовсім зрозуміла», сказав представник Facebook.

Ці примітивні емоції дозволяють провести більш кропіткий аналіз, чого не можна сказати про складні та зарозумілі схеми – важливий аргумент, чому прості класифікації переможуть складні. Письмові коментарі під статтею не дуже допомагають соцмережі. Складно визначити емоцію через те, що приведений текст можна трактувати не однозначно, звісно якщо це не «круто» чи «лол». У класифікації з шістьма емоціями існує багато переваг. Facebook, Buzzfeed та інші сервіси планують зробити реакції ще простішими. В різних країнах, мовах та культурах практично нема відмінностей в наборах реакцій на ту чи іншу новину.

Сентименти також допомагають аналізувати пости в кількісному відношенні. Користувачі власноруч сортують статті та відносять їх до категорій: «прекрасно», «смішно», «печально», «обурливо», «зворушливо».

Почитавши текстові відповіді, дуже складно визначити, що у новин «Канада зволікає з договором про торгівлю» і «поп-співак оголосив, що йде зі сцени» існує щось спільне. Але якщо вони обурять користувачів настільки, що ті нажмуть на кнопку «обурливо», Facebook зафіксує закономірність. Така класифікація дозволить Facebook пропонувати користувачам статті зі схожими реакціями або ж зробити таку собі добірку. Якщо реакції на статтю розділяться, Facebook зможе створити підкатегорію «кумедно та зворушливо» або «жахливо та обурливо». Сайт зможе відстежувати хто та як реагують на той чи інший допис, а потім спрогнозувати їх реакцію на майбутній контент.

Facebook здатен ізолювати сердитих людей та зменшити їх вплив на інших користувачів. Хоча ці шість реакцій не являються універсальним

набором, але той факт, що вони використовуються американською соцмережею зробив їх фактично стандартними. Якщо ми й далі будемо класифікувати наші реакції цими шістьма смайлами, Facebook і надалі буде оцінювати емоції в заданих рамках.

Мало хто знає, але набір емоцій був ще більшим. Повний список емоцій містив в собі схвалення, захоплення, гнів, жах та лють. Але весь спектр емоцій довелося скоротити, щоб він був більш універсальним та простішим для користування. Згідно з дослідженнями Дачера Келтнера (Dacher Keltner) країни, що виражали в більшості «щастя» не були щасливими насправді.

«Суть не в тому, щоб бути найщасливішими, а в тому, щоб відчути різні емоції» – сказав Келтнер.

Лімітований набір із шести реакцій сприяє звуженню емоційного різностороннього сприйняття подій. Соціальні мережі та рекламні компанії ставлять собі за мету викликати в людину ту чи іншу емоцію та зібрати статистику реакцій на свій продукт. Емоційний набір з шести емодзі, який запропонував Facebook – це мова, яку може зрозуміти комп'ютер. Мова основного набору емоційних реакцій зрозуміла як для людини, так і для машин. Вони нагадують більш прості таксономії Майерс-Бриггс або HEXACO, що розбивають складний феномен на класифікації. Реакції у Facebook чимось схожі на «Велику п'ятірку»:

Подобається: Доброзичливість;

Супер: Екстраверсія

Ух ти!: Відкритість

Печально: Невротизм

Обурливо: Сумлінність

Ви, мабуть, помітили, що тут немає «хаха». Ця емоція випадає із закономірності тому що сміх не піддається загальній класифікації, не дивлячись на те, що ця емоція є найпоширенішою серед юзерів. Інші п'ять емоцій згладжують наші культурні відмінності. Попри те, що Facebook намагається узагальнити ці шість реакцій, навряд вони означатимуть одне і те ж в різних куточках світу. Компанія підібрала різні емодзі, які будуть зрозумілі різним культурам. Якщо ці емоції попадуть у руки агрегатора даних, то ми незабаром усі в один голос будемо плакати, любити, охати від здивування тощо.

Мова реакцій – це примітивний набір емоцій, який набагато простіший за іноземні мови. Він більш зрозумілий машинам. Коли я розробляв графічні стікери для месенджера в 1999 році, я не міг це передбачити. В 2015 році я помічав зміни в новинній стрічці фейсбуку. Люди стали менше спілкуватися словами. Друзі все частіше коментували пости односкладно: «фу», «да» або ж просто вставляли смайли. Я сам став так відповідати їм.

Я проскролив свою стіну та звернув увагу на пости 2009 року. Я писав повними реченнями, аргументував свою думку кількома абзацами. Ці зміни були помітними. Різнобічність, нюанси та неоднозначність відійшли на другий план. Тепер користувачі більш стандартизовані. Ми вже говоримо іншою мовою. Мова Facebook – це мова комп'ютерів.

(вгору)

Додаток 8

12.09.2018

Черное зеркало: как побороть зависимость от соцсетей, пока не поздно

Насколько опасно повальное увлечение людей смартфонами? Ни для кого не секрет, что чрезмерное пользование гаджетами и социальными сетями ведет к разрушению социальных контактов и возникновению зависимости, однако ученые все еще не могут определить, существует ли в действительности эта зависимость (Politeka).

Действительно, каждый взрослый человек знает, что проводит в телефоне огромное количество времени, что игры после рабочего дня отнимают шансы прочесть интересную книгу, а недостаточное количество лайков под новым фото вызывает тревожность. Многие знаменитости заявляют, что «устают» от соцсетей, и устраивают себе «отпуск», а то и вовсе удаляют аккаунты. Сериалы «Мистер Робот» и «Черное зеркало» транслируют идею «во что мы все с вами превратились», но стали ли мы от этого хоть немного осознаннее?

По статистике EuroData 2017 года, около 42 % людей проверяют свои смартфоны в первые 10 минут после пробуждения. В этом году издание The Huffington Post, основанное Арианной Хаффингтон, выпустило совместно с Samsung приложение Thrive, которое позволяет гибко настраивать срочные оповещения и отключить ненужные. По словам журналистки, технологии до такой степени ускорили ритм нашей жизни, что «мы живем теперь будто лишь затем, чтобы обслуживать свои устройства, а вовсе не пользуемся ими как инструментами, облегчающими быт».

В январе инвестиционная компания Jana Partners, один из крупнейших акционеров Apple, выслала корпорации требование принять меры для помощи родителям, которые пытаются контролировать бесконечное «общение» своих детей со смартфонами. А профессор Университета Джеймса Мэдисона Нейт Маленке рассказывает, что его студенты кладут смартфоны на столы экранами вниз, «но легко заметить, что каждые две минуты они переворачивают их, чтобы взглянуть на обновления – будто какой-то невроз». Примечательно, что у самого Маленке никогда не было смартфона.

Ученые проводят массу социальных и других экспериментов, чтобы понять причину того, что смартфоны оказывают такое мощное влияние на нашу жизнь. Несмотря на то, что революционных открытий сделано не было, появились интересные результаты исследований, демонстрирующий как вред, так и пользу от жизни со смартфоном. В 2017 году статья в The Journal of the Association for Consumer Research сообщала, что чем дальше смартфон откладывался во время тестов на IQ и память, тем лучше был результат испытуемого, невзирая на то что во всех случаях аппараты переводили в бесшумный режим. Другие работы показали, что дружеский разговор без

смартфонов оставляет лучшее впечатление у всех участников (Misra et al., 2014) и что фотографирование шедевра искусства снижает вероятность сохранить о нем яркое воспоминание (Henkel, 2013). С другой стороны, нидерландские исследователи (Vossen, Valkenburg, 2016) обнаружили корреляцию между постоянным пользованием соцсетями и улучшением показателей в тестах на эмпатию у детей. А ученые из Китая (Lui, 2012) выяснили, что наиболее активные потребители медийного контента, привыкшие постоянно оперировать множеством источников информации, способны быстрее принимать бессознательные решения.

Почти каждому из нас присуща умеренная зависимость от собственных гаджетов: мы можем контролировать ее, но все равно испытываем тревожность, если к телефону или сети нет доступа. В качестве «лечения» специалисты рекомендуют оставлять телефон заряжаться ночью в соседней комнате, ограничивать время пользования определенными программами с помощью специальных приложений или переводить экран в черно-белый режим, чтобы уведомления не привлекали к себе внимание.

Не исключено, что социальные сети будут признаны не более опасными, нежели электричество или комиксы, которые пугали предыдущие поколения. Однако, они могут оказаться для общества чем-то вроде сахара в диете – привлекательной, но вредной добавкой.

Удалите самые «соблазняющие» приложения. Можете не слишком переживать: все данные наверняка сохранятся в облаке; настройте домашний Wi-Fi, ограничив время доступа в интернет; отправляйтесь в отпуск (оставьте смартфон дома); обратитесь к психологу, специалисту по лечению аддикций.

Марк Цукерберг, миллиардер и основатель социальной сети Facebook, в конце 2017 года пообещал, что виртуальная платформа снизит частоту показов «вирусных» видео, чтобы сократить время, которое пользователи соцсети тратят впустую. В свою очередь, компания Apple пообещала разработать более точные «родительские» настройки в своих девайсах.

Пользователи тоже не сидят без дела. Около 40 % норвежских студентов установили популярное приложение Hold, которое предлагает виртуальные награды за снижение активного пользования смартфоном.

Человечеству свойственно впадать в крайности – от непонимания и отторжения нового до одержимости им. Остается надеяться, что вскоре установится равновесие, которое даст технологиям развиваться, а человеческому обществу – существовать, не распадаясь. Тем более, что будущее готовит нам новые испытания: искусственный интеллект, беспилотные автомобили, дополненная реальность – возможно, тогда увлечение своими смартфонами уже не будет казаться нам серьезной проблемой.

(вгору)

Додаток 9

6.09.2018

Диктаторы заточили Facebook под себя
Ирина Фоменко

В прошлом месяце Facebook обнаружил доказательства скоординированной кампании влияния на своей платформе, во главе которых стоят иранские группы. Четвертого сентября несколько исследований пролили свет на другие способы, используемые правительствами в Facebook в ужасных целях: создание бригад влиятельных людей и платных армий троллей для подавления инакомыслия и отрицания реальности злодеяний в области прав человека. Об этом сообщает The Verge (InternetUA).

Журналисты The New York Times Деклан Уолш и Сулиман Али Звэй изучали, как «клавиатурные воины» Ливии используют Facebook для «охоты на врагов». «Вооруженные группы используют Facebook, чтобы найти противников и критиков, некоторые из которых впоследствии были задержаны, убиты или покинули страну. Преступные командиры сеют этническую ненависть. Распространяются фейковые документы, часто с целью подорвать работу национальных учреждений, например, Центрального банка», – пишут Уолш и Звэй.

«В The New York Times выяснили, что оружие военного класса продается открыто, несмотря на политику компании, запрещающую такую торговлю. Торговцы людьми используют свои страницы для расширения бизнеса. Практически каждая вооруженная группа в Ливии и даже некоторые из центров содержания под стражей имеют свою собственную страницу в Facebook», – сообщается в исследовании.

«На сегодняшний день самая опасная, грязная война ведется в социальных сетях и некоторых других медиа платформах. Ложь, фальсификация, вводящие в заблуждение факты. Электронные армии используют все. Это смертельная война», – заявил на прошлой неделе бывший министр информации Махмуд Шаммам.

Между тем на Филиппинах Дави Альба из BuzzFeed обнаружил, что автократ Родриго Дутерте считает Facebook очень эффективным для преследования инакомыслящих. С момента, как Дутерте занял свой пост, было совершено 12000 внесудебных казней, финансируемых государством. Трое приспешников Дутерте, одна из которых стала правительственным пресс-секретарем, координировали распространение дезинформации и преследовали политических оппонентов.

Завтрашние слушания в Конгрессе будут посвящены использованию странами технической платформы для сеяния раздора в Америке.

(вгору)

Додаток 10

5.09.2018

У соцмережах розгортається «гонка озброєнь» – операційний директор Facebook

Втручання Росії у виборчий процес в США було неприпустимим нападом на цінності країни, і компанія Facebook докладатиме зусиль, аби подібне не повторилося (InternetUA).

Про це заявила головний операційний директор Facebook Шеріл Сендберг під час слухань на тему використання платформ соціальних мереж в іноземних операціях впливу, які відбувалися 5 вересня у комітеті із розвідки Сенату Конгресу США, повідомляє власний кореспондент Укрінформу.

«Ми бачили, що може статися, коли наш сервіс використовують порушники (...) Ми реагували надто повільно. Це – наша провина. Втручання (Росії – ред.) було абсолютно неприпустимим. Воно було нападом на цінності нашої компанії і країни, яку ми любимо», – сказала вона стосовно втручання Росії у вибори президента США 2016 року.

Сендберг додала, що зараз Facebook докладає зусиль, які демонструють волю протистояти злочинним діям. Вона повідомила, що у липні було видалено 32 сторінки, які підозрювалися у «неприродній поведінці», у серпні – заблоковано 650 іранських сторінок і певна додаткова кількість російських, а лише минулого тижня – видалено 58 сторінок з М'янми.

«Америка завжди зазнавала нападів від цілеспрямованих і добре фінансованих опонентів, які хочуть підірвати нашу демократію. У цьому немає нічого нового, але тактика, яку вони використовують нині – нова. Нам треба працювати разом, аби не пасти задніх», – сказала вона, звертаючись до членів комітету. Сендберг додала, що росіяни теж не стоять на місці і поліпшують свої спроможності.

«Це гонка озброєнь», – сказала Сендберг, підсумовуючи свою доповідь.

Сендберг також поінформувала сенатський комітет, що Facebook докладає зусиль, аби запобігти можливому втручанню у проміжні вибори у США 6 листопада, а також в інших країнах. «Ми готуємося до проміжних виборів у США, які наближаються. А також до інших виборів у світі», – сказала вона.

На слуханнях у комітеті із розвідки Сенату Конгресу США на тему використання платформ соціальних мереж в іноземних операціях впливу були присутні головні виконавчі директори компаній Facebook та Twitter.

(вгору)

Додаток 11

5.09.2018

В Facebook рассказали, что подготовились к вмешательству в выборы

В интернет-компании Facebook подготовились к возможному иностранному вмешательству в выборы, в том числе в промежуточные выборы

в США, которые состоятся в ноябре 2018 года, рассказал американский телеканал NBC News (InternetUA).

В частности, в компании заявили о планах создать «оперативный штаб» – комнату, в которой будут оперативно координировать реакцию в режиме реального времени на зловредную интернет-активность во время промежуточных выборов в США, говорится в материале. Отмечается, что данные усилия выполняются по поручению генерального директора и основателя компании Марка Цукерберга.

Менеджер отдела по гражданской активности Facebook Самид Чакрабарти рассказал, что теперь пользователи социальной сети благодаря «политической прозрачности рекламы» могут видеть, кто стоит за рекламой и кто за нее заплатил.

«Я думаю, что это помогает создать гораздо более надежную среду для политического дискурса на наших платформах», – сказал Чакрабарти.

Представитель интернет-компании отметил, что действующие недобросовестно пользователи стали более изощренными – например, они научились лучше скрывать свое местоположение. Однако в Facebook сказали, что стали успешнее отслеживать случаи, когда люди пытаются скрыть свое местоположение. По словам сотрудника интернет-гиганта, Facebook в настоящее время «намного эффективнее, чем когда-либо».

Помимо этого, сотрудник интернет-компании добавил, что Facebook работает в этом направлении не один, а взаимодействует с правительствами по всему миру, а также экспертами по безопасности и гражданским обществом. Кроме того, Самид Чакрабарти рассказал, что компания увеличила штат, который работает для защиты пользовательских стандартов, с 10 тыс. человек в 2017 году до 20 тыс. человек в настоящее время. Все эти сотрудники занимаются различными вопросами, в том числе в этой команде есть работники, обученные разведкой, а также ученые, которые признаны одними из лучших в области вычислительных данных в мире, рассказали телеканалу.

(вгору)

Додаток 12

11.09.2018

Слежка за лайками. НАБУ хочет мониторить соцсети за 42 тысячи гривен

Виталий Губин

Национальное антикоррупционное бюро объявило о закупке услуг по мониторингу и анализу социальных сетей, а также по изучению медиа-активности в региональных СМИ, посвященных упоминаниям ведомства. Соответствующие заявки, датированные 6 сентября, размещены на портале публичных закупок Prozorro (Страна.UA).

Так, договор с претендентами на отслеживание контента в соцсетях НАБУ планирует заключить до конца 2018 года, предлагая за эту услугу 42 тысяч гривен.

Согласно заявленным техническим требованиям, на аукционе ведомство Артема Сытника планирует отобрать поставщика услуг, который будет в онлайн-режиме 24 часа в сутки семь дней в неделю предоставлять сведения по меньшей мере пяти темам, задаваемых для мониторингов, определенных заказчиком. Исполнитель должен будет предоставлять соответствующие услуги «в режиме, приближенном к реальному времени», с максимальной задержкой на час после появления конкретных постов. Основной упор в данной деятельности будет направлен на контент социальных сетей Facebook, Twitter, Instagram, Youtube и Telegram, а также на содержание блогов, форумов и тех сайтов, где наличествуют комментарии под публикациями.

От исполнителя потребуют предоставить результаты мониторинга неограниченному числу пользователей, позволить настраивать темы для изучения с помощью задавания выборки из ключевых слов. Результаты оперативного анализа должны будут отображаться в личном кабинете детективов НАБУ не позднее, чем за два часа с момента настройки фильтра по конкретной теме. В свою очередь, Бюро настаивает на своем исключительном праве неограниченное количество раз изменять темы для мониторинга в соцсетях путем уведомлений подрядчика, наличии опции по отбору и использованию «стоп-слов» для фильтрации конкретных упоминаний объекта мониторинга, а также возможность просмотра полной выборки результатов исследования в виде ретроспективных данных за 12 дней.

Перед поставщиком ставится условие обеспечения фильтрации сообщений по дате, тональности высказываний, географии, типу источника, а также автору и динамике проявленного им интереса к конкретной теме. Отдельно оговаривается также система оповещения НАБУ об «авральных ситуациях», например в части получения онлайн-уведомлений заказчика о «росте негатива» или знаковом сообщении от того или иного лидера общественного мнения, а также количестве охваченной конкретным постом или темой аудитории.

Что же касается второго лота планируемой закупки НАБУ, то перед этим поставщиком услуг ставятся более конкретные задачи, связанные с мониторингом 200 региональных СМИ согласно определенной выборке. Объектом изучения «мониторщиков» в данном случае будет выступать деятельность НАБУ и его территориальных управлений в регионах, а также выявление потенциально коррупционных деяний, подследственных ведомству Сытника. Впрочем, лотом также предусматривается отдельная настройка мониторингов на прочие темы и ключевые слова, которые могут меняться.

Данные онлайн-отчетов исполнителей, как и в случае с отслеживанием активности в соцсетях, также должны будут формироваться в режиме реального времени с возможностью доступа к их данным в режиме 24/7, возможность фильтрации их результатов по тональности материалов

(«позитив», «негатив», «нейтрально»), а также определение признаков заказного характера публикаций и присвоения репутационных рисков конкретным сюжетам.

Предполагается, что исследованию будут подлежать 4-5 телеканалов в Харькове, Одессе и Львове (с возможностью ситуативного дополнительного мониторинга «телевизоров» конкретной области), не менее десяти печатных СМИ на каждую область, а также 100 сайтов. От претендентов на оказание такого рода услуг в НАБУ требуют предоставить в тестовом режиме дайджест и онлайн-мониторинг. Предполагаемый срок заключения договорных обязательств между Бюро и подрядчиком по этому лоту исчерпывается 31 декабря 2018 года, а заявленная стоимость закупки составляет 120 тысяч гривен.

(вгору)

Додаток 13

13.09.2018

Начальник спецотдела ФСБ рассказал ФБР о работе российских ботов

Игорь Козлов

12 сентября в федеральном суде Хартфорда (столица штата Коннектикут) дал признательные показания гражданин России Петр Левашов. 38-летний житель Санкт-Петербурга обвинялся в намеренном повреждении защищенного компьютера, преступном сговоре и хищении личных данных с отягчающими обстоятельствами (Факты).

Американские СМИ акцентируют внимание на необычности этого дела. Левашов отличается от прочих российских хакеров, которых в США осудили уже немало. ФБР гонялось за ним на протяжении нескольких лет, кропотливо собирая улики. 20 мая 2016 года федералы получили доступ к аккаунту Петра в iCloud (облачное хранилище данных), открытому на его имя с IP-адреса в Люксембурге. Федеральный суд Аляски выдал ордер, обязавший корпорацию Apple, предоставить ФБР возможность взломать аккаунт Левашова и, одновременно, запрещающий компании разглашать любую информацию об этом.

Агенты ФБР получили необходимые им данные. После этого им оставалось ждать, когда Левашов окажется в одной из стран, власти которой согласятся выдать его США.

Такой страной оказалась Испания. 7 апреля 2017 года россиянин был задержан в Барселоне по американскому ордеру. Его экстрадировали в феврале. Кроме Коннектикута ему предъявили обвинения в еще нескольких американских штатах, а также Федеральном округе Колумбия.

В чем необычность дела Левашова? Начнем с того, что Петр, защищаясь в испанском суде, который принимал решение о его выдаче США, заявил, что является «офицером российской армии». Он утверждал также следующее: «Я

давал подписку о неразглашении, у меня секретная военно-учетная специальность. В течение последних 10 лет я работал на “Единую Россию”, собирал различную информацию про оппозиционные партии и занимался доведением этой информации до нужных людей в нужное время».

В связи с этим Левашов просил не выдавать его американским властям. «В США меня подвергнут пыткам, будут насильно вводить наркотики, чтобы получить информацию. Если я окажусь в США, то в течение года расстанусь с жизнью, там хотят получить информацию военного характера и про «Единую Россию», – заявил петербуржец испанскому судье.

Попав в США, Левашов резко изменил тактику. Он больше не упоминал ФСБ и не жаловался не пытки. Адвокаты рекомендовали ему сотрудничать с американскими властями. При этом официально ни одна из сторон факт сотрудничества не признает. Но СМИ отмечают множество косвенных доказательств того, что Левашов заговорил и предоставляемая им информация имеет ценность.

Доступ журналистам к большинству документов дела закрыт. Судья Роберт Чатиньи, несмотря на признание обвиняемого, заявил, что вынесет приговор в сентябре 2019 года, то есть через год. Видимо, ФБР потребуется время, чтобы разобраться в том, что им рассказал Левашов.

Что же все-таки совершил этот россиянин? Прокурор во время суда в Хартфорде заявил, что Левашов, известный также как Питер Севера и Сергей Астахов, «более двух десятилетий управлял ботнетами, участвовал в форумах, на которых торговали похищенными личными данными, реквизитами кредитных карт и орудиями киберпреступлений, жил при этом припеваючи, а между тем его преступная деятельность портила жизнь тысячам компьютерных пользователей».

ФБР заинтересовалось Левашовым из-за его огромного ботнета Kelihos, который позволял россиянину похищать чужие логины и пароли, рассылать неимоверное количество спама и запускать вирусы в чужие компьютеры по всему миру.

В момент ареста Левашова, заявил прокурор, Kelihos инфицировал не менее 50 тысяч компьютеров. Работу ботнета Министерству юстиции США удалось прекратить только после ареста Петра в Барселоне.

(вгору)

Додаток 14

17.09.2018

СБУ допомагатиме «Укренерго» та «Укргідроенерго» у кіберзахисті

Служба безпеки України підписала меморандум з енергетичною компанією «Укренерго» та ПАТ «Укргідроенерго» для ефективної системи кібербезпеки (Espreso.tv).

Про це повідомляє прес-служба СБУ.

Зазначається, що документ має забезпечити обмін інформацією з СБУ щодо кібернетичних загроз з використанням платформи MISP-UA зі стратегічно важливими підприємствами енергетичної галузі України.

«Обмін матеріалами, зокрема технологічною інформацією про реалізовані та потенційні кіберзагрози відбуватиметься в режимі реального часу. Така міжвідомча взаємодія сприятиме ефективному реагуванню з боку української спецслужби на кібернетичні атаки, насамперед високого ступеня складності», – заявили у відомстві.

Протягом останніх 5 років спостерігається еволюція різновидів кібератак на Україну, які все частіше набувають ознаки кібершпигунства та кібертероризму. Зафіксовано зростання активності спецслужб РФ щодо проведення цілеспрямованих кібератак, орієнтованих на отримання несанкціонованого доступу до інформаційних систем органів української держвлади. Здійснення акцій кібернетичного тероризму спрямовані, також, на порушення штатного функціонування комп'ютерних мереж та систем керування технологічними процесами об'єктів критичної інфраструктури.

У відомстві наголосили, що Ситуаційний центр забезпечення кібербезпеки готовий і надалі надавати захист не тільки об'єктам критичної інфраструктури, державним установам та підприємствам.

«Будь-який представник великого, середнього та навіть малого бізнесу може звернутися до центру за консультаціями та допомогою», – наголосив Голова СБУ Василь Грицак.

Крім того, працівники Ситуаційного центру на базі платформи з відкритим програмним кодом MISP, створили систему збору і обробки інформації щодо інцидентів кібербезпеки та обміну технічними даними об'єктів критичної інфраструктури з СБУ в режимі реального часу.

Зазначається, що ця платформа широко використовується в усьому світі, а також відповідає міжнародним стандартам ЄС та НАТО і застосовується основними міжнародними суб'єктами у сфері кібербезпеки FIRST, CIRCL, CiviCERT, NATO NCI Agency.

(вгору)

Додаток 15

17.09.2018

В Росії все частіше саджають за репости в Мережі, – Курносова

В Росії збільшилася кількість кримінальних та адміністративних справ за репости та дописи у соцмережі. Якщо раніше саджали за підтримку України, то наразі – за критику чинної влади (Аргумент).

Про це розповіла російський опозиційний політик, політична мігрантка Ольга Курносова під час прес-конференції в прес-центрі «Главком». В Росії є поліцейська дубина у вигляді кримінального законодавства. «Її можуть застосовувати так як хочеться силовикам або представникам органів влади. Тому ми бачимо, що весь час існування 282 статті Кримінального Кодексу РФ

за екстремізм, активно застосовується. Адже наразі вона містить так звані інтернет-поправки. Вони з'явилися у червні 2014 року. А перше читання цього документу відбулося ще у 2013 році. Звичайно, те, що ці поправки були прийняті саме у 2014 році, має місце український слід. Адже деякі росіяни активно підтримували Україну», – говорить Курносова. За її підрахунками, у 2014 році було відкрито 267 кримінальних справ, у 2015 році – 278, у 2016 – 395, 2017 – 465 кримінальних справ і 4 046 – адміністративних справ. «Не зрозуміло, навіщо тут застосовувати кримінальну статтю. У цій статті є не тільки серйозні штрафи, а й позбавлення волі від 2 років до 5. Тобто за репост у соцмережі якогось анекдоту або якоїсь картинки можна сісти в тюрму до п'яти років. І на жаль, сьогодні в Росії за репост можна отримати реальний вирок позбавлення волі», – продовжує Курносова.

Саджають не тільки по 282 статті кримінального Кодексу РФ. Також застосовують 280 статтю за виправдання екстремізму, а також статті за розпалювання почуття віруючих, реабілітацію нацизму. «Застосовують це все лише за те, що люди сьогодні критикують владу. Влада вважає, що вона є соціальною групою. А там є формулювання «за розпалювання ворожнечі в соціальній групі». Хоча є рішення Верховного Суду РФ про те, що не можна порушувати кримінальну справу за 282 статтею за критику чинної влади, тим не менш це рішення Суду ігнорується. Є смішна справа: одному губернатору на картинці намалювали «гітлерівські» вуса, і все, це вже розцінено як екстремізм, бо порівняли з нацистами представників влади», – підсумувала політична мігрантка.

(вгору)

Додаток 16

5.09.2018
В Google Play обнаружены сразу несколько банковских троянов

Банкеры

Только на прошлой неделе специалисты «Доктор Веб» рассказали об удалении из официального каталога приложений Google 127 вредоносов, и вот уже подоспели новые сообщения о малвари в Google Play. На этот раз специалисты по информационной безопасности обнаружили в каталоге сразу несколько семейств банковских троянов (InternetUA).

Так, 4 сентября эксперт компании ESET Лукаш Стефанко (Lukas Stefanko) рассказал у себя в Twitter о трех банкерах, которые маскировались под астрологические приложения и насчитывали более 1500 установок. Сейчас все три угрозы уже удалены из Google Play, но до этого приложения воровали SMS-сообщения и журналы звонков, могли отправлять сообщения от имени жертв, загружали и устанавливали сторонние приложения без одобрения владельца устройства, а также похищали банковские учетные данные.

Одно из найденных специалистом приложений (Herobot) прибегало к интересной маскировке. Оно показывало жертвам фальшивые предупреждения

о несовместимости и якобы удалялось, но на самом деле малварь продолжала работать в фоновом режиме и атаковала банковские приложения, установленные на устройстве. По данным Стефанко, управляющий сервер этого вредоноса активен до сих пор.

Эксперт отмечает, что все три банкера были опасны и из-за очень низкого уровня обнаружения антивирусными продуктами. На скриншотах ниже можно увидеть, что еще вчера, 3 сентября 2018 года, малварь обнаруживали максимум 12 решений из 60, представленных на VirusTotal.

Однако Стефанко – не единственный, кто сообщил о банковских троянах в Google Play за последние дни. О похожей находке в Twitter рассказал и специалист компании Avast Николаос Крисайдос (Nikolaos Chrysaidos).

Крисайдос нашел в каталоге приложений более пяти банкеров, выдававших себя из приложения для оптимизации производительности. По информации специалиста, данная кампания была активна с начала августа 2018 года.

Другие угрозы

К сожалению, в Google Play можно встретить не только банковские трояны, но и другие опасные приложения, которые могут угрожать пользователям как напрямую, так и косвенно.

К примеру, на прошлой неделе все тот же Лукаш Стефанко раскритиковал популярнейшее VPN-приложение Protect Your Data, которое может похвастаться более чем 10000000 установок. Исследователь предупреждал, что приложение следит за трафиком пользователей, собирает данные о местоположении, установленных и запущенных приложениях, а также о посещенных сайтах.

Другое приложение, под названием Transparent clock & weather, насчитывает более 50000000 установок и написано так плохо, что каждые 15 секунд передает вовне данные о местоположении пользователя в незашифрованном виде.

(вгору)

Додаток 17

6.09.2018

Официальное приложение для iPhone обманом списывало $100 в неделю

Мошенническое приложение Ancestry, которое маскировалось под реальную компанию с таким же названием, обманом заставляло пользователей покупать премиум-версию, эксплуатируя механизм подтверждения платежей с помощью отпечатка пальца на устройствах Apple. Приложение распространялось через официальный AppStore (InternetUA).

Мошенническое приложение

В AppStore было обнаружено приложение, которое мошенническим способом заставляет пользователей приобретать подписку на платную версию,

используя механизм подтверждение платежей с помощью отпечатка пальца на устройствах Apple. Приложение называется Ancestry, оно предназначено якобы для прослеживания генеалогической линии пользователя и поиска его родственников. На мошенническую подоплеку происходящего обратили внимание пользователи ресурса Reddit.

При регистрации Ancestry требует ввести имя, фамилию, год и место рождения. Затем под предлогом поиска биологических родственников приложение просит пользователя оставить в базе отпечаток пальца. Чтобы сформировать образец отпечатка, пользователю нужно несколько раз подряд нажать пальцем на кнопку.

Внезапно после очередного нажатия Ancestry выводит на экран предложение о покупке премиум-версии, еженедельная плата за которую составляет $100. Пользователь не успевает среагировать на изменения на экране и очередной раз нажимает на кнопку. Но это нажатие уже расценивается устройством Apple как подтверждение платежа. К настоящему моменту Apple успела удалить мошенническое приложение из AppStore.

Реальная Ancestry

Мошенники замаскировали свое приложение под продукт реально существующей компании Ancestry, которая занимается восстановлением генеалогического древа и поиском родственников по ДНК. В качестве логотипа реальная Ancestry использует стилизованное изображение зеленого листика, который злоумышленники заменили на розовое дерево.

Настоящая Ancestry – это частная компания, основанная в 1983 г. и базирующаяся в Лехи, штат Юта. Сначала компания занималась публикацией журнала Ancestry и генеалогических книг. Как подписочный сервис поиска родственников по ДНК она начала работать в 1997 г. после приобретения компанией Infobases. В 2009 г. Ancestry стала публичной компанией, но в 2012 г. снова перешла в частные руки.

В 2011 г. Ancestry запустила приложения для Android и iOS. Компания утверждает, что по состоянию на 2018 г. в ее потребительской ДНК-сети насчитывается более 10 млн человек, что делает ее крупнейшей в мире. Сервис Ancestry доступен почти в 30 странах.

(вгору)

Додаток 18

6.09.2018

У Chrome знайшли баг, який робить «дірявими» мережі Wi-Fi

Для успішного проведення атаки необхідно зробити один клік. Вразливість стосується усіх заснованих на Chromium браузерів, таких як Google Chrome, Opera, Slimjet, Torch та інших (TechToday).

Щоб вкрасти приватні дані з бездротової мережі Wi-Fi, зловмиснику не потрібно відгадувати її складний пароль – досить, щоб хтось із підключених

юзерів користувався браузером Chrome. Вразливість також існує у всіх браузерах, заснованих на Chrome, з Opera включно.

Дослідники з компанії комп'ютерної безпеки SureCloud виявили, що проблема полягає у тому, як хромоподібні браузери обробляють збережені паролі та передають їх у мережах Wi-Fi. За замовчуванням браузери зберігають логін та пароль для веб-сторінки адміністрування роутера Wi-Fi. Оскільки більшість роутерів не використовують шифрування в засобах налаштування, зловмисники можуть використати отримані реєстраційні дані, щоб перехопити роутер під свій контроль та видобути пароль мережі Wi-Fi.

Для успішного проведення атаки необхідно зробити один клік. Вразливість стосується усіх заснованих на Chromium браузерів, таких як Google Chrome, Opera, Slimjet, Torch та інших. Також вразливі всі роутери, у яких сторінка адміністрування передається по протоколу HTTP.

Дослідники віднайшли «діру» ще в березні 2018 року, і тоді ж повідомили розробників проекту Google Chromium. Однак ті в той самий день сказали, що це не баг, а функція, і браузер працює, як задумувалося. Планів щодо змін цієї функції немає.

Експерти рекомендують посилити захист своєї мережі тим, що заходити в консоль управління свого роутера Wi-Fi для налаштування чи інсталяції апдейтів за допомогою окремого браузера. Також вони говорять, що можна використовувати режим «інкогніто». Додатково варто очистити збережені паролі в браузері та не зберігати їх для сторінок HTTP. Окрім цього, варто видалити всі збережені мережі Wi-Fi без паролів, заборонити автоматичне підключення до мереж та змінити паролі Wi-Fi і доступу в консоль роутера.

(вгору)

Додаток 19

10.09.2018
Ирина Фоменко
Популярнейшее приложение на Mac работает как шпионское ПО

Приложение для проверки безопасности Adware Doctor в настоящее время занимает четвертое место в списке популярных приложений для Mac App Store. Но после появления видеоролика Privacy 1st с доказательством подозрительной работы программы, исследователи безопасности Mac Патрик Уордл из Digita Security и Томас Рид из Malwarebytes проанализировали ее, пишет Wired (InternetUA).

Исследователи обнаружили, что Adware Doctor собирает данные о своих пользователях, в частности историю просмотров и список других программ и процессов, запущенных на компьютере, сохраняет данные в заблокированном файле и периодически отправляет их на сервер, который, по-видимому, находится в Китае. Все эти действия нарушают правила App Store, но даже после уведомления Privacy 1st Apple о проблемах, приложение все еще находится в App Store.

«К сожалению, App Store действительно не является безопасным. Мы обнаруживаем и отслеживаем несколько различных подозрительных приложений в App Store. Некоторые из них удаляют быстро, а другие – по полгода. Это не просто вредоносная программа, а программное обеспечение, которое крадет ваши данные», – заявил Рид.

Когда пользователь загружает Adware Doctor, приложение запрашивает разрешение на доступ к папке MacOS «Home». Уордл обнаружил, что, как только Adware Doctor получит это разрешение, оно начинает собирать пользовательские данные, нарушая конфиденциальность и правила Apple.

Приложения Mac изолированы друг от друга и от операционной системы в контейнерах, так называемых «sandboxes», которые не позволяют программам получать доступ к другим. Adware Doctor использует разрешения, предоставленные ему для сбора данных, а затем находит способы обойти защиту изолированной среды. Так, программа пытается получить информацию о программном обеспечении, запущенном на компьютере пользователя.

Некоторые программы, например, антивирусы, используют эту возможность безопасно и законно, но приложения из App Store не должны иметь такой доступ. И хотя у macOS уже есть встроенная защита, Adware Doctor может собрать список запущенных программ и процессов через интерфейс прикладного программирования. Код, используемый Adware Doctor для составления списка запущенных процессов, взят из примеров, которые Apple публикует как часть своей документации.

В Malwarebytes начали отслеживать Adware Doctor в 2015 году, когда приложение называлось Adware Medic. Malwarebytes уведомили Apple, и компания удалила приложение, но затем оно снова появилось в App Store в течение нескольких дней как Adware Doctor.

Malwarebytes продолжали отслеживать приложение на протяжении многих лет, считая его подозрительным, поскольку его функциональность была ограничена – защита основана на открытом исходном коде. Но новые данные Privacy of 1st показывают, что приложение, возможно, недавно добавило расширенные подозрительные функции через обновление.

Adware Doctor позиционирует себя как продукт безопасности, чтобы казаться более надежным и получить системные разрешения. Однако Apple не разрешает публикацию большинства законных антивирусов в App Store, так как они требуют доступ к системе и могут не соответствовать более жестким требованиям.

После публикации видео Privacy 1st на прошлой неделе приложение переместили на сервер, который получал данные пользователя в автономном режиме. Однако Adware Doctor по-прежнему пытается отправить информацию.

«То, как Apple реагирует в этой ситуации – довольно плохо, поскольку Adware Doctor является самым продаваемым приложением в App Store, а Apple получает прибыль от каждой программы», – прокомментировал Уордл.

Несмотря на то, что публикация вредоносных приложений не является беспрецедентной в App Store, это необычно для такой программы, которую

постоянно отслеживают. И это важное напоминание о том, что при загрузке нового программного обеспечения всегда существует определенный риск.

(вгору)

Додаток 20

11.09.2018

Хакеры PowerPool используют в целевых атаках уязвимость нулевого дня

ESET предупреждает о целевых атаках с использованием новой, пока не закрытой производителем уязвимости в Microsoft Windows. По данным телеметрии, атаки нацелены на пользователей в России, Украине, Польше, Германии, Великобритании, США, Индии, Чили и на Филиппинах (Компьютерное Обозрение).

Уязвимость представляет собой локальное повышение привилегий (Local Privilege Escalation), которое позволит выполнять вредоносный код с максимальными правами. Баг связан с работой Планировщика задач Windows и затрагивает версии операционной системы Microsoft Windows с 7 по 10.

Информация об уязвимости нулевого дня была раскрыта 27 августа. На момент публикации обновления безопасности отсутствовали.

Всего через два дня после публикации специалисты ESET обнаружили, что эксплойт к новой уязвимости используется в целевых атаках кибергруппы PowerPool. Хакеры несколько изменили опубликованный на GitHub код эксплойта и перекомпилировали его.

Атака начинается с рассылки вредоносных спам-писем с бэкдором первого этапа. Вредоносная программа предназначена для базовой разведки в системе – она выполняет команды атакующих и передает собранные данные на удаленный сервер.

Если компьютер заинтересовал хакеров, на нем будет установлен бэкдор второго этапа, обеспечивающий постоянный доступ к системе. Далее операторы PowerPool использует уязвимость нулевого дня для повышения привилегий. Для перемещения внутри скомпрометированной сети атакующие используют инструменты с открытым исходным кодом: PowerDump, PowerSploit, SMBExec, Quarks PwDump, FireMaster.

Атаки PowerPool нацелены на ограниченное число пользователей. Тем не менее, инцидент показывает, что злоумышленники отслеживают тренды и оперативно внедряют новые эксплойты. Раскрытие информации об уязвимостях до выхода обновлений безопасности может послужить причиной массовых кибератак.

(вгору)

Додаток 21

14.09.2018

Каждая четвертая кибератака нацелена на частных лиц

По данным Positive Technologies за II квартал, количество инцидентов кибербезопасности выросло на 47 % по сравнению с прошлогодним. При этом доля целевых атак превысила долю массовых и составила 54 % (Компьютерное Обозрение).

Продолжила расти доля атак, выполненных с целью получения конфиденциальной информации. Злоумышленники больше всего были заинтересованы в персональных (31 %) и учетных данных (22 %), в том числе в паролях от онлайн-банков частных лиц. Их похищали главным образом посредством компрометации различных онлайн-площадок – интернет-магазинов, сервисов для продажи билетов, бронирования отелей и т.п.

Во второй половине квартала произошло большое количество атак на криптовалютные сети, такие как Verge, Monacoin, Bitcoin Gold, ZenCash, Litecoin Cash. В результате злоумышленники похитили в общей сложности более 100 млн долл. Доля подобных атак также выросла по сравнению с аналогичным периодом прошлого года.

Что касается методов атак, лидерство по-прежнему удерживают атаки с применением вредоносного ПО, несмотря на то что во II квартале 2018 г. доля атак, в которых злоумышленники использовали вредоносное ПО, сократилась (49 % вместо 63 % в I квартале). При этом существенно выросла доля других методов атак, например, эксплуатация веб-уязвимостей (18 % вместо 12 %) и подбор учетных данных (19 % вместо 7 %).

Доля атак на веб-ресурсы выросла и составила 32 % вместо 23 %. По сравнению с I кварталом выросла и доля атак на IoT-устройства. По мнению экспертов, это преимущественно связано с появлением новых ботнетов, таких как PyRoMineIoT, Muhstik, Wicked Mirai.

Государственные организации продолжают оставаться излюбленной мишенью для киберпреступников, при этом злоумышленников в первую очередь интересует коммерческая тайна, например, зарплатные ведомости, трудовые договора и любые другие документы ограниченного доступа.

По итогам кибератак, жертвами которых во II квартале стали частные пользователи, ущерб составил десятки миллионов долларов, а число пострадавших составило 765 млн.

Тенденция к увеличению доли атак, направленных на хищение данных, вероятно, сохранится, считают в компании. Многие компании уделяют недостаточно внимания защите обрабатываемой информации, что делает ее легкой добычей даже для низкоквалифицированных хакеров. Полученные данные затем продаются на теневом рынке.

(вгору)

Додаток 22

16.09.2018

Как посты в соцсетях могут помешать получить кредит

Банки, страховые компании и продавцы техники уже давно используют так называемый скоринг по соцсетям, чтобы принять решение об одобрении кредита человеку или об осуществлении для него других операций. Людей просто проверяют. Таким образом кредиторы или страховщики понимают, что вы не лгали о работе, доходах и семейном положении. The Daily Mail написал целую статью о методах работы западных финансистов. UBR.ua заинтересовался ими, поскольку украинские банки часто заимствуют опыт иностранных коллег и все быстрее внедряют их технологии (InternetUA).

В ней отмечается, что если человек дает согласие на то, чтобы финучреждение проанализировало его активность в соцсетях, специальные компании, например FriendlyScore и Hello Soda соберут для подобных учреждений всю информацию. Исполнительный директор FriendlyScore Лабна Базин говорит, что анализ проводится с помощью машин, ни один человек не увидит, чем вы делитесь в сети. При этом представители финансового комьюнити уже высказывали недовольство по поводу нарушения приватности.

Согласиться на то, чтобы банк «проскорил» ваши профили в интернете, вы можете путем настроек учетной записи или загрузив специальное приложение. Процесс скоринга используется для того, чтобы финучреждения понимали, сможете ли вы вовремя выплатить кредит.

Что именно могут увидеть?

К примеру в Твиттере робот посмотрит на то, кого вы фолловите и на то, чем вы делитесь, чтобы понять ваши интересы. В Gmail проследят, какие письма вы получаете от онлайн-магазинов, чтобы понять, как вы тратите свои деньги. На LinkedIn «пинкертон» проверит, говорили ли вы правду по поводу истории своей занятости и квалификации. С помощью мобильного приложения банк или страховая получит доступ к местам, которые вы посещаете, где вы живете и где работаете. Также приложение получит доступ к контактам в вашем телефоне и советует хранить данные о кредитоспособных друзьях и семье на вашем телефоне.

Такой способ определения финансовой состоятельности не всегда корректен: заявка на кредит может быть отклонена несправедливо только на основании того, какое шоу вы любите или покупаете еду или вещи в определенном супермаркете, соответственно, эта же модель работает и в противоположном направлении.

Что делать, чтоб защититься от тренда скоринга через соцсети?

1.Убедитесь, что то, о чем вы говорили в интернете, не противоречит тому, что вы указали в кредитной или страховой заявке. Хорошо подумайте перед тем, как давать доступ к своим соцсетям.

2.Следите за сайтами, которые используют ваш Facebook, Twitter или другие учетные записи для входа. Вы можете дать им доступ ко всем видам своих персональных данных и контактов, которые хранятся в этих учетных записях.

3.Настройте Facebook так, чтобы только друзья могли видеть ваши публикации.

4.Не храните в своем списке контактов людей, у которых были проблемы с выплатой кредитов.

(вгору)

Додаток 23

17.09.2018

Как понять, что вашу переписку кто-то читает

Использует ли кто-то посторонний ваши аккаунты? Почти во всех сервисах это можно проверить за пару кликов. Мы собрали инструкции для самых популярных соцсетей, почтовых сервисов и мессенджеров. Они пригодятся тем, кто сомневается в конфиденциальности своей переписки, и тем, кому просто любопытно (InternetUA).

Google

Аккаунт Google предлагает две возможности, связанные с безопасностью. Можно просмотреть список недавно использованных устройств за последние 28 дней. Если какое-то устройство покажется вам незнакомым, вы сможете закрыть для него доступ к аккаунту.

Как найти: Аккаунт Google > Безопасность и вход > Недавно использованные устройства

Еще возможно увидеть все предупреждения системы безопасности и список действий, связанных с сохранностью ваших данных (например, попытки изменить пароль или параметры восстановления доступа к аккаунту). Сервис позволяет видеть IP-адрес, время, местоположение и браузер, связанные с каждый действием.

Как найти: Аккаунт Google > Безопасность и вход > Недавние события

Facebook

В настройках десктопной версии соцсеть покажет вам все устройства, браузеры, IP-адреса, а также координаты входов за последний год. Сессии на подозрительных устройствах можно завершить.

Как найти: Настройки > Безопасность и вход > Откуда вы вошли

Instagram

Соцсеть покажет вам все входы в аккаунт с момента регистрации, а также выходы, смены пароля и изменения уровня конфиденциальности. Вот только принадлежат ли эти входы вам, узнать не получится. Поэтому в случае приступа паранойи Instagram ничем не сможет вам помочь.

Как найти: Страница профиля в десктопной версии > Настройки > Конфиденциальность и безопасность > Данные аккаунта > Действия > Входы

Viber

Мессенджер Viber позволяет изучить список всех устройств, на которых работает ваша учетная запись и когда ей в последний раз пользовались. Все лишнее легко можно отключить.

Как найти: Мобильное приложение > Настройки > Учетная запись > Компьютеры и планшеты

Telegram

Мессенджер в два клика покажет все активные сеансы – те устройства, на которых в ваш аккаунт вошли и не вышли. Можно прервать как один подозрительный сеанс, так и все, кроме текущего.

Как найти: Настройки > Конфиденциальность и безопасность > Показать все сеансы

Skype

Ничего похожего на список активных устройств в Skype мы не нашли. Похоже, этот сервис не позволяет отследить, читает ли вашу переписку кто-то посторонний. Но выход есть: в любой сомнительной ситуации достаточно просто сменить пароль.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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